Informationele zelfbeschikking in de zorg

Hooghiemstra, Theo

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

Informationele zelfbeschikking in de zorg

Informationele zelfbeschikking in de zorg

Proefschrift

ter verkrijging van de graad van doctor
aan Tilburg University
op gezag van de rector magnificus, prof. dr. E.H.L. Aarts,
in het openbaar te verdedigen ten overstaan van een
door het college voor promoties aangewezen commissie
in de aula van de Universiteit op maandag 2 juli 2018
om 16.00 uur

door

Theodorus Franciscus Maria Hooghiemstra
geboren te Beek gemeente Bergh

Promotores:	Prof.mr. J.E.J. Prins Prof.mr.dr. P.C. Ippel
Promotiecommissie:	Prof.mr.dr. L.H.J. Adams Dr.mr. C.M.K.C. Cuijpers Prof.mr.dr. H. Franken Dr.mr. S. Nouwt Prof.dr. C. Stuurman

Vormgeving omslag: Villa Y, Den Haag

Van deze studie is een handelseditie verschenen bij Sdu Uitgevers bv onder

ISBN: 978 90 1240 236 1

Inhoudsopgave

Lijst van gebruikte afkortingen

AABvRvS	Afdeling Bestuursrechtspraak van de Raad van State
AAID	Accountability and Internet Democracy
ADR	Alternative dispute resolution
A-G	Advocaat-Generaal
AIVD	Algemene Inlichtingen en Veiligheidsdienst
AMvB	Algemene Maatregel van Bestuur
AP	Autoriteit persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BES	Bonaire, St Eustatius en Saba
BIG	Beroepen individuele gezondheidszorg
BKR	Bureau Kredietregistratie
BSN	Burgerservicenummer
BverfG	Bundesverfassungsgericht
BOPZ	Bijzondere opnemingen in psychiatrische ziekenhuizen
BW	Burgerlijk Wetboek
CBP	College Bescherming Persoonsgegevens
CEG	Centrum voor Ethiek en Gezondheid
CTG	Centraal Tuchtcollege voor de gezondheidszorg
DBC	Diagnose Behandel Combinatie
DIS	DBC-Informatiesysteem
DPA's	Data Protection Authorities
DPIA	Data Protection Privacy Impact Assessment
ECG	Elektrocardiogram (hartfilmpje)
ECRM	Europese Commissie voor de Rechten van de Mens
EHRM	Europees Hof voor de Rechten van de Mens
EPD	Elektronisch patiëntendossier
EU	Europese Unie

EVRM	Europees Verdrag tot bescherming van de rechten van de mens en de Fundamentele vrijheden
FDA	Food and Drug Administration
FG	Functionaris Gegevensbescherming
FMS	Federatie Medisch Specialisten (FMS)
GfK	Gesellschaft für Kommunikationsforschung
GG	Grundgesetz
GGZ	Geestelijke Gezondheidszorg
GPS	Global Positioning System
Handvest	Handvest van de Grondrechten van de Europese Unie
HBU	Hollandse Bank Unie
HiiL	Hague Institute for Innovation of Law
HEC	Het Expertise Centrum
ICT	Informatie- en communicatietechnologie
IGJ	Inspectie Gezondheidszorg en Jeugd
Ineen	Organisaties in de Eerste Lijn
HR	Hoge Raad der Nederlanden
HvJ EU	Hof van Justitie van de EU
KNGF	Koninklijk Nederlands Genootschap voor Fysiotherapie
KNMG	Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst
KNMP	Koninklijke Nederlandse Maatschappij ter bevordering der Pharmacie
LHV	Landelijke Huisartsen Vereniging
LSP	Landelijk Schakelpunt
mHealth	Mobile Health
MvT	Memorie van Toelichting
NeLL	Nationaal eHealth Living Lab
NFU	Nederlandse Federatie van Universitair Medische Centra
NHG	Nederlands Huisartsen Genootschap
NJ	Nederlandse Jurisprudentie
NJCM	Nederlands Juristen Comité voor de Mensenrechten
NJV	Nederlandse Juristen Vereniging
NSA	National Security Agency
NVZ	Nederlandse Vereniging van Ziekenhuizen

NZa	Nederlandse zorgautoriteit
ODR	Online dispute resolution
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
OM	Openbaar Ministerie
PET	Privacy enhancing technologies
PG	Procureur-generaal
PGO	Persoonlijke Gezondheidsomgeving
P&I	Privacy & Informatie
PVP	Patiëntenvertrouwenspersoon
Rb.	Rechtbank
R.o.	Rechtsoverweging
ROM	Routine Outcome Monitoring
RTG	Regionaal Tuchtcollege voor de gezondheidszorg
RVS	Raad voor Volksgezondheid en Samenleving
RVZ	Raad voor de Volksgezondheid en Zorg
SBG	Stichting Benchmark GGZ
SGOA	Stichting Geschillenoplossing Organisatie & Automatisering
Sr	Wetboek van Strafrecht
Stb	Staatsblad
Stcrt.	Staatscourant
Sv	Wetboek van Strafvordering
TvCR	Tijdschrift voor Constitutioneel Recht
TvGr	Tijdschrift voor Gezondheidsrecht
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
UMCG	Universitair Medisch Centrum Groningen
UVRM	Universele Verklaring voor de Rechten van de Mens
VGN	Vereniging Gehandicaptenzorg Nederland
VIPP	Versnellingsprogramma Informatie-uitwisseling Patiënt & Professional
VNG	Vereniging van Nederlandse Gemeenten
VoIP	Voice-over-Internet-Protocol (bellen over een computernetwerk/internet)
VPH	Vereniging voor Praktijkhoudende Huisartsen
VwEU	Verdrag betreffende de werking van de Europese Unie

VWS	Volksgezondheid, Welzijn en Sport
VZVZ	Vereniging van Zorgaanbieders voor Zorgcommunicatie
Wabvpz	Wet aanvullende bepalingen verwerking van persoonsgegevens in de zorg
Wbp	Wet bescherming persoonsgegevens
Wet BIG	Wet op de beroepen in de individuele gezondheidszorg
Wet RO	Wet Rechterlijke Organisatie
WGBO	Wet op de geneeskundige behandelingsovereenkomst (art. 7:446 e.v. BW)
Wiv	Wet op de inlichtingen- en veiligheidsdiensten
Wkkgz	Wet kwaliteit, klachten en geschillen zorg
WP29	Working Party 29 (artikel 29 werkgroep van de gezamenlijke DPA's)
Zvw	Zorgverzekeringswet

Voorwoord

Gedurende een lange periode heb ik aan deze dissertatie mogen werken, met als voordeel dat mijn gedachten en ideeën zich hebben kunnen ordenen en ontwikkelen. Een ander voordeel is dat vraagstukken rondom het onderwerp 'Informationele zelfbeschikking in de zorg' inmiddels zeer actueel zijn. Ook in de zorg is er sprake van snelle informatietechnologische ontwikkelingen en een intensief juridisch en maatschappelijk debat over de machtsvraag rond persoonsgegevens.

De totstandkoming van de dissertatie heb ik te danken aan velen die mij hebben bijgestaan of hebben geïnspireerd. In de eerste plaats mijn promotor professor Pieter Ippel die mij motiveerde om dit onderzoek aan de hand van mijn intellectuele passie te beginnen. Aanvankelijk met als thema 'Gradaties van zelfbeschikking'. Dat deze dissertatie er nu ook echt ligt, is vooral te danken aan de discipline, precisie en toegewijdheid van mijn andere promotor, professor Corien Prins.

In de privésfeer dank ik mijn naasten, paranimfen, familie en vrienden die me de benodigde tijd hebben gegund en mij stimuleerden om dit werk af te maken.

Ook dank ik mijn collega's bij HEC/PBLQ en de RVZ/RVS die mij op allerlei manieren hebben gesteund.

In mijn dankwoord aan het einde van dit boek heb ik geprobeerd de vele personen die mij hebben geholpen, bij naam te noemen.

Den Haag, mei 2018

1 *Introductie*

1.1 CONTEXT

Informatie- en communicatietechnologie (ICT) biedt de belofte van een uitgebreid aanbod aan faciliteiten voor personen[1], met voor sommige als ideaal 'volledige informationele zelfbeschikking'. In deze dissertatie staat dit ideaal centraal en wel vanuit de focus of en zo ja voor wie en onder welke voorwaarden informationele zelfbeschikking *in de zorg* een na te streven ideaal is. De specifieke inkleuring van deze focus en de daaruit voortvloeiende onderzoeksvraag komen verderop aan de orde. Allereerst start deze inleiding met een korte schets van de context waarin de thematiek wordt onderzocht.

'Informationele zelfbeschikking' is te definiëren als:

> *"Het vermogen van een persoon om in beginsel zelf te bepalen in hoeverre persoonsgegevens worden gebruikt en verder bekendgemaakt, met het oog op een zelfbepaald leven".*[2]

Cardioloog en geneticus Topol voorspelt in zijn boek *The Patiënt will see you now*[3] dat de smartphone de controle over medische gegevens direct bij personen zal brengen.
Zelf besefte Topol dat zijn wereld veranderd was toen hij op een dag een e-mail kreeg van een patiënt met boezemfibrillatie, die een 'doe-het-zelf-elektrocardiogram' bij zijn mail had gevoegd via een hulpstuk bij zijn slimme telefoon. Een patiënt kan zelf al een ECG[4] maken via zijn smartphone en daarbij ook nog eens een interpretatie krijgen van een computer, waarna de dokter kan nagaan of de computer gelijk heeft. Dat betekent dat de rol van de zorgaanbieder[5] in en rond de behandeling drastisch verandert.
Maar niet alleen de rol van de zorgaanbieder, ook die van personen gaat veranderen, volgens Topol. Zij krijgen met de smartphone en andere apparaten (horloge

1. Synoniem voor: individu, gebruiker, betrokkene, patiënt, cliënt, zorgconsument en werknemer.
2. Deze definitie is een combinatie van de uitspraak door het Bundesverfassungsgericht. (Constitutioneel Hof) 15 december 1983, BVerfGE, 65, 1 (43); 78, 77 (84); 84, 192 (194); 113, 29 (46); 115, 166 (188); 115, 320 (341f.); 117, 202; BVerwG, NJW 2008, 3081; BayVerfGH, DVBI, 2003,861; HambOVG, DÖV 2007,893 (Ls); SächsOVG, NJW 2007,169 (170); BGH, BGHZ 171, 252 (256), de opvatting van Rouvroy en Poullet, in Gutwirth e.a., 2009. p. 51 en inzichten opgedaan bij het schrijven van deze dissertatie.
3. Topol 2015.
4. Elektrocardiogram (hartfilmpje).
5. Een instelling dan wel een solistisch werkende zorgverlener (overeenkomstig artikel 1 Wet kwaliteit, klachten en geschillen zorg – Wkkgz).

en andere *wearables*[6]) immers voor het eerst een instrument in handen om zelf hun gezondheid te monitoren en beheren. De smartphone geeft hen toegang tot medische informatie. Deze medische informatie is veelal te kwalificeren als gezondheidsgegevens in de zin van de Algemene verordening gegevensbescherming (AVG).[7] Volgens artikel 9 AVG gaat het bij 'gegevens over gezondheid' om 'persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven'.
Overweging 35 van de AVG voegt wat betreft de term gezondheidsgegevens daar aan toe dat het omvat: 'alle gegevens (…) die betrekking hebben op de gezondheidstoestand van een betrokkene en die informatie geven over de lichamelijke of geestelijke gezondheidstoestand van de betrokkene in het verleden, het heden en de toekomst'. In concreto kan de voorspelling van Topol betekenen dat onze smartphones en andere mobiele apparaten in toenemende mate gezondheidsgegevens zullen verwerken. Personen kunnen dan zelf bepalen of ze deze gegevens willen delen met hun arts, andere zorgverleners of mensen en organisaties buiten de zorgcontext.
In zijn boek geeft Topol een reeks van toepassingen die deze ontwikkeling illustreren. Een *app*[8], bijvoorbeeld, om via de microfoon onze ademhaling digitaal te analyseren of onze longfuncties te meten. Een 'elektronische neus', om via een ademhalingsanalyse bepaalde types van kanker op te sporen. Of een miniatuurlaboratorium dat als aanhangsel van een smartphone razendsnel zeer kleine hoeveelheden bloed, urine of speeksel kan analyseren. Aan zogenoemde 'labs on a chip' wordt hard gewerkt. Dit kan ertoe leiden dat we in de toekomst een gepersonaliseerd en gedigitaliseerd profiel van onze gezondheid bij ons zullen dragen, aldus Topol.

De hierboven geschetste ontwikkeling geeft personen een gepersonaliseerd en gedigitaliseerd profiel van hun gezondheid. Het lijkt te passen in het streven van het Informatieberaad Zorg[9] om via het programma 'MedMij' persoonlijke gezondheidsomgevingen[10] een prominente plek te laten innemen in de Nederlandse zorg. Het Afsprakenstelsel MedMij maakt onderdeel uit van dit programma.[11] Dit streven naar een persoonlijke gezondheidsomgeving is overeenkomstig het eerdere advies 'Patiënteninformatie' van de Raad voor de

6. *Wearables* zijn gadgets die op het lichaam gedragen kunnen worden en verbonden zijn met een computer. Bijvoorbeeld horloges (*smartwatches*), maar ook bijvoorbeeld brillen (*Google Glass*) en sokken die snelheid, afstand en calorieverbruik meten.
7. Verordening (EU) 2016/679. Zie verder 5.3.6 voor de AVG en 6.2.2 voor de Uitvoeringswet AVG.
8. Een *app* is een klein computerprogramma bestemd voor een smartphone of tablet zoals een iPhone of iPad. Met een *app* kan er een bepaalde activiteit worden uitgevoerd. Zo worden *apps* vaak gebruikt om mee te bankieren, muziek te downloaden, naar de radio te luisteren of te chatten. Ook ten behoeve van het bijhouden van gezondheidsgegevens zijn er steeds meer gezondheidsapps. Wereldwijd ongeveer 350.000. Zie verder hoofdstuk 2.
9. https://www.informatieberaadzorg.nl/.
10. Op 19 maart 2018 maakte minister Bruins van VWS bekend dat tot de zomer van 2018 door partijen in de zorg, gesubsidieerd door VWS, een proef wordt gestart met persoonlijke gezondheidsomgevingen https://nos.nl/artikel/2223291-zorgpartijen-patienten-kunnen-straks-allerlei-medische-gegevens-inzien.html.
11. Zie www.medmij.nl.

Volksgezondheid en Zorg (RVZ)[12], waarin het – onder voorwaarden – stimuleren van een persoonlijk gezondheidsdossier (PGD)[13] werd bepleit.

Programma MedMij kiest voor het begrip persoonlijke gezondheidsomgeving[14] in plaats van persoonlijk gezondheidsdossier. Op www.medmij.nl wordt een persoonlijke gezondheidsomgeving als volgt gedefinieerd:

> *"Een persoonlijke gezondheidsomgeving is een digitale omgeving die je in staat stelt om al je relevante gezondheidsgegevens, die verspreid liggen opgeslagen bij professionele zorgverleners, zorgaanbiedersinstellingen en overheden, in te zien, aan te vullen met zelf gegenereerde gegevens en te delen met wie je dat wilt. Persoonlijke gezondheidsomgevingen bieden via* websites *en* apps *toegang aan alle gezondheidsgegevens van de betreffende persoon."*

In deze dissertatie zal de nodige aandacht worden besteed aan de praktijk rondom een persoonlijke gezondheidsomgeving. Een persoonlijke gezondheidsomgeving is een concrete invulling van informationele zelfbeschikking. Dit onderzoek richt zich niet alleen op regulering van technologische en maatschappelijke trends die personen via gegevensgebruik meer zelfbeschikking geven, maar besteedt nadrukkelijk ook aandacht aan de praktische uitvoerbaarheid van de te stellen normen. In dit verband zullen ook andere vormen van regulering dan alleen wetgeving in beeld komen. Ook vormen van maatschappelijke verantwoord ondernemen bij zorginstellingen en bedrijven, als voorbeeld van geconditioneerde zelfregulering, behoren tot het palet aan mogelijkheden om invulling te geven aan het streven ompersonen meer zelfbeschikking te geven. In de combinatie van theorie en praktijk, maakt het onderhavige onderzoek mede gebruik van eigen empirisch onderzoek[15] als ook secundair[16], bestaand onderzoek en overzichten van technologische ontwikkelingen.[17] Zo is dankbaar gebruik gemaakt van onderzoeksrapporten van HEC/PBLQ, de RVZ/RVS, de WRR, NIVEL, ZonMw en TNO. Belangrijk bij de analyse in deze dissertatie van deze en andere praktijkervaringen is de overtuiging dat de rol van regulering vooral ook aan de voorkant van de ontwikkelingen in beeld dient te komen en niet uitsluitend als een soort van sluitpost als de toepassingen vorm hebben gekregen. Deze dissertatie is er daarom mede op gericht een passend moreel-juridisch kader te ontwikkelen

12. RVZ, 2014.
13. Zie de definitie van J. Wolter en M.W. Dolan, *The Personal Health Record*. Chicago IL: AHIMA, American Health Information Management Association, geciteerd in R.J. Barelds, e.a., *Het Persoonlijk Gezondheidsdossier. Een foto van het PGD in Nederland*. TNO rapport KvL/P&Z 2009.109. In opdracht van Nictiz. December 2009. Vgl. ook R.A.E. Gerards, T.F.M. Hooghiemstra, A.G. Arnold, A.D. van der Heide, *De informatiepositie van de patiënt*. Papernote 31. HEC, Sdu Uitgevers 2010 en het daarop gebaseerde en gelijknamige artikel van T. Hooghiemstra en R. Gerads in *Privacy & Informatie*, 2010, 51. Zie ook T.F.M. Hooghiemstra en J. Nouwt, 'eHealth en recht. Inleiding op het thema'. In: *Computerrecht: Tijdschrift voor informatica, telecommunicatie en recht*, 6/2011, p. 289 en Hooghiemstra, T.F.M., *Zelfbeschikking bij ICT en het medisch dossier*. Privacy & Informatie 2007.
14. Voorheen werd de naam Persoonlijk Gezondheidsdossier (PGD) gehanteerd. Om het verschil te benadrukken met Elektronische Patiënten Dossiers is voor het begrip 'Persoonlijke Gezondheidsomgeving' gekozen.
15. Zie de speciaal voor dit onderzoek uitgevoerde empirische studie door CentERdata van de Universiteit Tilburg: https://www.centerdata.nl/sites/default/files/bestanden/achtergrondstudie_recht_op_informationele_zelfbeschikking_in_de_zorg.pdf.
16. O.a TNO (2015), Privacybeleving op het internet in Nederland.
17. Zie bijvoorbeeld: http://uk.businessinsider.com/internet-of-everything-2015-bi-2014-12?r=US&IR=T. zie, Moerel & Prins 2016.

voor gezondheidsgerelateerde applicaties die individuen een vorm van informationele zelfbeschikking beogen te geven.

1.2 MEER CONTROLE EN ZELFBESCHIKKING VOOR PERSONEN

De huidige samenleving kent onder meer als kenmerkende trend dat actoren steeds meer hechten aan individuele controle en zelfbeschikking als tegenkracht. Bij velen vertaalt deze tendens zich in de behoefte aan meer zelfbeschikking bij het verzamelen en beheer van gegevens, waaronder gezondheidsgegevens. De technologie faciliteert deze tendens in sterke mate, zoals bij persoonlijke gezondheidsomgevingen die rechtstreeks aan de persoon worden aangeboden door marktpartijen zonder tussenkomst van zorgverleners. Veelal wordt in dit verband de term 'consumenten eHealth'[18] gebruikt. Overigens kenmerkt de huidige samenleving zich door meer tendensen, zoals: demografische veranderingen, verschuiving van economische macht, verstedelijking, klimaatverandering, tendensen in de technologie en social media. Tussen de tendens dat actoren meer hechten aan individuele controle en zelfbeschikking en informationele zelfbeschikking bestaat een duidelijke relatie. Ook in de zorg is dit duidelijk, zo zal uit dit onderzoek blijken.

In hoofdstuk 2 wordt nader ingegaan op de specifieke technologieën die individuen meer mogelijkheden bieden om het heft in eigen handen te nemen wat betreft inzicht in en controle op de eigen gezondheid. Op deze plaats kan ter agendering van de thematiek op een drietal voorbeelden worden gewezen. Op 31 juli 2016 lanceerde Philips vijf nieuwe consumenten eHealth toepassingen, gecertificeerd door de Food and Drug Administration (FDA) en verbonden met de centrale mobiele app Philips *HealthSuite*. Het betreft diensten voor personen om aan preventie en management te doen voor diabetes, hartziekten en andere chronische ziekten. In hoofdstuk 2 worden deze diensten van Philips *HealthSuite* nader toegelicht.
Een tweede voorbeeld betreft het bericht in de *New York Daily* van 7 augustus 2016, waarin melding wordt gemaakt van de claim door IBM dat het met zijn IBM Watson AI-platform in staat is om in tien minuten met de juiste diagnose te komen van een zeldzame vorm van leukemie bij een 60-jarige Japanse vrouw, waar menselijke specialisten deze diagnose niet konden stellen. Als laatste voorbeeld valt te wijzen op de door Philips tezamen met American Well op 9 januari 2018 gepresenteerde uGrow-app voor ouderschap (gepresenteerd op de Consumer Electronics Show (CES) in Las Vegas). Met uGrow kunnen ouders onder meer gegevens delen met – en gepersonaliseerd advies ontvangen van – beroepsbeoefenaren in de gezondheidszorg. Met hulp van American Well biedt de app een beveiligde, on-demand videoverbinding met een kinderarts, medische arts of specialist in geestelijke gezondheidszorg online of via de mobiele telefoon, 24 uur per dag, 7 dagen per week. Voor de service betalen consumenten een vergoeding die verschilt per zorgprofessional en consultatie-

18. RVZ, 2015.

duur. Philips en American Well gaan veel meer zeer gepersonaliseerde virtuele zorgoplossingen aan consumenten en zorgprofessionals leveren.[19]

Bovengenoemde toepassingen bieden personen ongekende nieuwe mogelijkheden, maar vanuit het oogpunt van informationele zelfbeschikking zijn er zeker ook de nodige risico's en beperkingen. Nieuwe technologieën maken het mogelijk om steeds grotere datasets te verzamelen, op te slaan en te koppelen. Dit fenomeen wordt *big data* genoemd. De datasets maken van de persoon niet alleen een gebruiker van een big-datatechnologie, maar tevens ook een databron. De kracht van het fenomeen *big data*[20] schuilt in de combinatie van een aantal ontwikkelingen, zoals[21] de exponentiële groei in beschikbare gegevens en de steeds grotere rekencapaciteit met behulp van analyse-algoritmen. De schaduwzijden – maar ook beloften van *big data* – zullen eveneens in hoofdstuk 2 worden benoemd.

1.3 ONDERZOEKSVRAGEN

De hier aangestipte maatschappelijke en technologische trends tonen in ieder geval dat er meer aandacht is en mogelijkheden zijn voor informationele zelfbeschikking van personen. Dat roept de vraag op hoe deze ontwikkeling, meer in het bijzonder gerelateerd aan informationele zelfbeschikking, zich verhoudt tot het vigerende wettelijk kader voor de omgang met persoonsgegevens. Daarmee komt een belangrijke vraag voor dit onderzoek in beeld: in hoeverre is het bestaande wettelijk kader passend voor de aangestipte trends? Aan de hand van het antwoord op deze vraag moet vervolgens worden bezien of normatieve en feitelijke overwegingen noodzaken tot een aanpassing van de bestaande wet- en regelgeving. Bij het beantwoorden van deze vragen laat ik me inspireren door rechtsfilosofen, zoals Fuller, Selznick, Berlin en Nissenbaum. Vanuit de theorievorming die door hen is ontwikkeld, kan worden vastgesteld in hoeverre aanvullende regulering gewenst is met het oog op het waarborgen van fundamentele rechten die mede gestoeld zijn op het belang van menselijke waardigheid. Concreet levert deze globaal geformuleerde ambitie de volgende vier clusters van onderzoeksvragen voor deze dissertatie op:

I Wat dient, mede in het licht van technologische ontwikkelingen, te worden verstaan onder informationele zelfbeschikking? Is informationele zelfbeschikking mogelijk en wenselijk, in hoeverre en met welke beperkingen? Kan en moet daarbij onderscheid worden gemaakt naar typen personen?
II Wat betekent een en ander concreet voor de – ook historisch gegroeide en ontwikkelde – uitwerking van informationele zelfbeschikking via regulering?
III Normering kan ook gestalte krijgen in de applicaties zelf, namelijk via *privacy-by-design*. Deze en andere mogelijkheden kunnen in potentie personen faciliteren bij het beheer van hun gezondheidsgegevens. Maar wat betekent dit concreet op het terrein van gezondheid en gezondheidszorg?
IV Welke overige toekomstgerichte aanbevelingen zijn er – gelet op de opmars van persoonlijke gezondheidsomgevingen – te geven om informationele zelfbeschikking te realiseren?

19. https://www.ed.nl/philips/philips-gaat-samenwerking-aan-met-american-well~ad5940b3/.
20. Zie onder andere het preadvies van de Vereniging voor Gezondheidsrecht, 2017.
21. Moerel & Prins 2016.

1.4 INKADERING VAN HET ONDERZOEK

Het concept van informationele zelfbeschikking is als zodanig niet nieuw, maar wordt in dit onderzoek in een ander perspectief geplaatst. Van passieve/defensieve zelfbeschikking bij het destijds door het Duitse Constitutioneel Hof omschreven recht voor personen om in beginsel zelf te beschikken over persoonsgegevens[22] naar een actief/offensief recht waarbij personen zelf controle kunnen uitoefenen over hun gegevens met behulp van ICT.[23] Het onderzoek richt zich primair op de Nederlandse situatie, maar laat zich daarbij inspireren door de Duitse en Europese begripshistorie, dogmatiek en jurisprudentie. Als uitwerking van het begrip 'informationele zelfbeschikking' komen ook de begrippen 'privacy' en 'bescherming van persoonsgegevens' in dit onderzoek aan de orde.[24] De wortels van privacy – meer precies het recht op privéleven – en de bescherming van persoonsgegevens liggen in de concepten van menselijke waardigheid en autonomie. Dit impliceert ook het recht van iedere persoon om zijn eigen persoonlijkheid te ontwikkelen en zelfbeschikking te hebben over zaken die direct op hem van invloed zijn.[25] In Duitsland is uit concepten van menselijke waardigheid en autonomie ook de grondslag voor informationele zelfbeschikking af te leiden. In Europa is het recht op privacy (privéleven) neergelegd in artikel 8 van het Europees Verdrag voor Rechten van de Mens en de fundamentele vrijheden (EVRM) van 1950 en artikel 7 Handvest van de grondrechten van de Europese Unie (Lissabon, 2007[26]). In Europa is het recht op bescherming van persoonsgegevens neergelegd in het verdrag van de Raad van Europa onder de naam 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (CETS No. 108, Verdrag van Straatsburg, 1981), Richtlijn 95/46/EG (1995) en artikel 8 van het Handvest van de grondrechten van de Europese Unie. De AVG is sinds 25 mei 2018 van toepassing.[27]

Dit onderzoek focust zich op het streven naar regie van personen over hun eigen gezondheid via een persoonlijke gezondheidsomgeving. Binnen de context van een persoonlijke gezondheidsomgeving speelt natuurlijk de vraag wat de reikwijdte van het zorgdomein is, juist omdat de applicaties faciliteren dat gegevens over de grenzen van contexten (care, cure, sociaal domein) heen worden benut. Vertrekpunt in deze dissertatie zijn de bestaande elektronische uitwisselingssystemen met dossiers van zorgverleners[28] en zorgaanbieders overeenkomstig de Wet op de geneeskundige behandelingsovereenkomst

22. Bundesverfassungsgericht, 15 december 1983, BVerfGE, 65, 1 (43).
23. Overigens blijkt uit de paragrafen 173 t/m 175 van het Bundesverfassungsrecht van 1983 inzake 'informationelle Selbstbestimmung' dat het recht op informationele zelfbeschikking geen absoluut recht kan zijn en genuanceerd is.
24. Zie o.a. Hustinx 1999, 2005, 2013 en 2017.
25. Zie Hustinx, 2017, p.124.
26. Zie Verdrag van Lissabon, 13 december 2007.
27. Zie artikel 99 van de Verordening (EU) 2016/679.
28. Overeenkomstig artikel 1 van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) wordt in deze dissertatie onder een zorgaanbieder verstaan: "een instelling dan wel een solistisch werkende zorgverlener" en onder een zorgverlener "een natuurlijke persoon die beroepsmatig zorg verleent".

(WGBO)[29] en de Wet aanvullende bepalingen voor verwerking van persoonsgegevens in de zorg (Wabvpz)[30]. Personen kunnen vervolgens in hun persoonlijke gezondheidsomgeving zelf deze gegevens (laten) opnemen en aanvullen met andere gegevens over hun gezondheid. In deze dissertatie vallen andere domeinen dan de aldus gedefinieerde gezondheidszorg (zoals het sociaal domein[31]) buiten de scope van het onderzoek.

De volgende vier aandachtspunten worden vanuit het voorgaande in dit onderzoek verondersteld.

In de eerste plaats beperkt de kwetsbare positie van veel personen hun zelfbeschikking. Vanuit het oogpunt van menselijke waardigheid is het van belang dat de overheid enerzijds partijen de ruimte geeft in het invulling geven aan zelfbeschikking en anderzijds randvoorwaarden stelt.
In de tweede plaats gaat het in dit onderzoek om informationele zelfbeschikking en niet om zelfbeschikking in de volle breedte. Dit betekent dat de bescherming van persoonsgegevens in beeld komt.
In de derde plaats is in de relatie patiënt-zorgverlener gedeelde besluitvorming (*shared decision making*, oftewel: gezamenlijke besluitvorming) een samenspel tussen zorgverlener en patiënt. Een context waarin patiënten voortdurend hun rechten poneren, schuurt met de maatschappelijke werkelijkheid. Overigens wordt in de geneeskundige literatuur *shared decision making* juist vaak gezien als een stap op weg richting meer zelfbeschikking voor de patiënt en een evenwichtigere arts-patiëntrelatie.[32]
In de vierde plaats zijn er juridische, technologische en organisatorische randvoorwaarden noodzakelijk gelet op hoe de markt en posities van partijen op die markt zich in de alledaagse praktijk ontwikkelen. Vanwege de snelheid van die ontwikkelingen en het patiëntgerichte perspectief bij informationele zelfbeschikking is responsieve regulering, in de geest van Nonet en Selznick, evenals de sociale theorie van Selznick hiervoor een belangrijke inspiratiebron.

1.5 NORMATIEF KADER

1.5.1 Inleiding

Het normatieve kader van dit onderzoek wordt uitgewerkt aan de hand van het werk van Fuller, Selznick, Berlin en Nissenbaum. Fuller[33] en Selznick[34] hebben beiden het ideaal ontwikkeld dat "wetgevers het perspectief moeten innemen van degenen die met de regels moeten werken en leven".[35] Fuller hanteert een

29. In de zin van artikel 446 en volgende boek 7 Burgerlijk Wetboek.
30. *Stb.* 2017/279.
31. Zie bijvoorbeeld de brief van de minister van VWS over het medisch beroepsgeheim (21-12-2017), waarin nadrukkelijk ook aandacht is voor het gebruik van zorggegevens binnen andere domeinen dan de zorg (waaronder sociaal domein), https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/21/kamerbrief-over-acties-verbetering-informatiepositie-privacy-medisch-beroepsgeheim.
32. Zie Elwyn, 2012 en 2015, Makoul 2006, Mulley 2012, Stiggelbout 2012 en 2015, Vermunt 2017.
33. Fuller 1969, p. 39-40.
34. Selznick 1992, p. 373.
35. Witteveen 2014, p. 456 en Moerel & Prins 2016. p. 18.

dynamisch rechtsbegrip. Volgens Fuller is recht '*the enterprise of subjecting human conduct to the governance of rules*'.[36] De door hem genoemde '*internal morality of law*' geeft kwaliteitseisen voor wet- en regelgeving vanuit het perspectief van recht als proces.

De visie van Fuller en Selznick past binnen mijn overtuiging dat het normatieve kader recht moet doen aan de complexiteit van de technologische en maatschappelijke werkelijkheid.

Een belangrijk element in dit normatieve kader is het ideaal van *responsieve regulering*.[37] Het ideaal van responsieve regulering wordt gecombineerd met de overtuiging dat personen in het huidige informatietechnologische tijdperk de garantie dienen te hebben dat informationele zelfbeschikking voor degenen die dit kunnen of willen, daadwerkelijk effectief is. In de digitale wereld kan niet volstaan worden met een juridische bescherming die is gestoeld op het klassieke uitgangspunt ten aanzien van fundamentele rechten dat de overheid de burger met rust moet laten. Als blijkt dat de overheid voor een realistische bescherming van individuen een actieve in plaats van passieve rol heeft te vervullen, dan dient ze zich daarvoor sterk te maken.[38] Ik haak hierbij aan op het raamwerk in het preadvies van 2016 voor de NJV van Moerel en Prins, dat gebaseerd is op de *capability approach* van Nobelprijswinnaar Sen.[39] Verder valt uit de rechtspraak inzake artikel 8 EVRM van het Europese Hof voor de Rechten van de Mens af te leiden dat de lidstaten niet alleen een onthoudingsplicht hebben, maar ook een zorgplicht: zij moeten het grondrecht actief beschermen. Bovendien is er nog het vraagstuk van de botsing van grondrechten, zoals artikel 8 versus artikel 10 EVRM.[40]

In het kader van het liberalisme-communitarisme debat maakte Berlin in zijn essay '*Twee opvattingen van vrijheid*' een belangwekkend onderscheid tussen positieve en negatieve vrijheid. Bij negatieve vrijheid gaat het om een afperking van het eigen domein, waar de Staat en anderen zich niet in mogen mengen. Hier staat centraal: Vrij zijn van iets te moeten doen dat anderen je opleggen. Anders gezegd: Het gaat vooral om een afweerrecht, om zelfbeschikking over de eigen persoonlijke levenssfeer. Hoewel Berlin toegeeft dat dit een beperkte opvatting is, acht hij deze conceptueel helder en daarom bruikbaar in een politieke en morele discussie.

Bij positieve vrijheid gaat het om 'vrijheid tot'. De beschikbaarheid van kansen om de 'auteur van je leven' te zijn en het leven betekenisvol te maken.[41] Positieve vrijheid vraagt juist om stimulering door anderen om zelfbeschikking daadwerkelijk mogelijk te maken. Berlin waarschuwde dat een begrip als positieve vrijheid (dit geldt bijvoorbeeld ook voor een attractief klinkend begrip als 'actief burgerschap') het gevaar van ideologisch misbruik en van politieke manipulatie op kan roepen. Er is een tendens om 'mogen' al snel in 'moeten' te transformeren, om een recht om te zetten in een plicht, onder de hoede van

36. Fuller 1969, p. 106.
37. Zie ook: Dorbeck-Jung 2015, p. 24.
38. Maurits Martijn & Dimitri Tokmetzis, 2016, laten zien dat privacy het meest bedreigde mensenrecht van onze tijd is.
39. Sen, A., 1984.
40. Zie Nieuwenhuis, Den Heijer & Hins, 2014.
41. Berlin 1958.

een zogenaamd 'zorgende' overheid of zorgverzekeraar. Mogelijkheden kunnen verplichtingen worden. Zo is bijvoorbeeld denkbaar dat onder de vlag van deze idealen personen wegens bezuinigingsdoeleinden of gemakzucht verplicht worden gesteld hun gegevens te gaan beheren, oftewel administratief werk uit te besteden. In de consumentenwereld van vliegen, reizen en verblijven is dit vaak al het geval. Of en in hoeverre dit in de praktijk ook bij 'informationele zelfbeschikking' het geval kan zijn, wordt later in dit onderzoek uitgewerkt. Naar analogie kan gesteld worden dat informationele zelfbeschikking een aantrekkelijke gedachte is, maar als ideologie kan leiden tot misbruik of oneigenlijke druk. Nissenbaum wijst erop dat sommige bedrijven meer macht hebben dan Staten.[42] Wat betreft de overheden zijn de beginselen van goede *governance* en het staatsrecht belangrijk om onderdrukkende krachten in toom te houden.
De centrale stelling van Nissenbaum is dat mensen een privacyschending kunnen ervaren bij partijen die informatie verzamelen, analyseren of verspreiden omdat die bepaalde normen over de informatiestroom overschrijden. Mensen ervaren volgens Nissenbaum bij partijen geen privacyschendingomdat zij het gevoel hebben dat ze de controle kwijtraken of de geheimhouding wordt geschonden. De informatiestroom heeft een onderwerp, is van een bepaald type en wordt onder bepaalde voorwaarden geuit. Als een van deze 'normen' verandert dan is de informatiestroom niet meer gepast. Bij contextuele integriteit wordt het doel van een bepaalde context sociaal geconstrueerd. Bij dit onderzoek gaat het om de zorgcontext. Een kernvraag is of de kernelementen van deze context beschermd moeten kunnen worden of beschermd kunnen blijven als personen hun persoonsgegevens laten beheren door partijen die geen medische hulpverleners zijn. Zoals bij persoonlijke gezondheidsomgevingen in het licht van de maatschappelijke en technologische ontwikkelingen die in hoofdstuk 2 aan bod komen. In hoofdstuk 3 wordt deze vraag verder uitgewerkt.
Het begrip '*contextuele integriteit*'[43] is een inspiratiebron voor Nissenbaum.[44] Nissenbaum legt het accent niet op de individuele rechten om 'eigen' gegevens te kunnen controleren, maar op de noodzaak te zorgen dat er geschikte stromen van persoonlijke informatie zijn. Wat geschikt is, komt voort uit de contextuele integriteit. Op conceptueel niveau is geschiktheid geassocieerd met context en norm. Een recht op privacy is noch een recht op geheimhouding, noch een recht op controle, maar een recht op een geschikte stroom van persoonlijke informatie. Voor volledige privacy moet men volgens Nissenbaum in een grot leven.
Binnen de huidige wet- en regelgeving inzake de bescherming van persoonsgegevens worden informatierechten juist als hoeksteen beschouwd.[45] De veronderstelling daarbij is dat een persoon ook daadwerkelijk zijn recht kan uitoefenen, omdat hij weet dat er informatie over hem wordt verwerkt en door wie. De AVG gaat door op die ingeslagen weg en versterkt de informatieverplichtingen en de rechten van individuen, ook vanuit de gedachte dat dit bijdraagt aan de informationele zelfbeschikking van het individu en hem meer controle biedt over

42. Nissenbaum 2010.
43. Walzer 1983. Met contextuele integriteit wordt hier bedoeld: Intellectueel instrument waarmee antwoord kan worden gevonden op de vraag waarom een bepaalde context als zeer bedreigend voor privacy wordt ervaren en in een andere niet.
44. Nissenbaum 2010.
45. Nissenbaum 2010, p.90 e.v.

gegevensverwerking. Dit uitgangspunt is ook te vinden in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz).[46] Zowel de AVG als de Wabvpz bevat onder andere het recht van personen op elektronische inzage van hun gegevens, het recht op een elektronisch afschrift van hun gegevens en het recht op een elektronisch afschrift van de logbestanden. In logbestanden wordt vastgelegd wie het elektronische dossier heeft geraadpleegd. Met deze nieuwe rechten krijgen personen meer informationele zelfbeschikking. Volledige eigen zelfbeschikking over gezondheidsgegevens lijkt binnen de zorg om uiteenlopende redenen meestal niet wenselijk. Wie leest de volledige gebruiksvoorwaarden bij bijvoorbeeld gezondheidsapps? Wat is het alternatief voor 'Op Akkoord' klikken? In hoeverre bevinden zieke, kwetsbare personen zich in de positie om echt vrijwillig en goed geïnformeerde toestemming te geven?

1.5.2 Theorieën van Nonet en Selznick

De sociale theorie van de Amerikaanse rechtssocioloog en -filosoof Selznick is anno 2016 nog steeds relevant bij een analyse van de huidige ontwikkelingen in technologie en samenleving, omdat hij het liberale ideaal van vrijheid verbindt met de noodzaak van een nieuw institutioneel ontwerp.[47]
Informationele zelfbeschikking in de zorg moet er niet toe leiden dat personen versnipperd als bits[48] ieder voor zich bezig zijn met hun persoonlijke gezondheidsomgeving in een wereld van machtige bedrijven en overheden. Een nieuw institutioneel ontwerp om personen te beschermen en in de praktijk werkelijk zo veel mogelijk echte informationele zelfbeschikking te geven, is noodzakelijk. Over het lot van de mens in een wereld waarin digitale techniek en 'het net' diens bestaan fundamenteel veranderen, laat Schnitzler in '*Het Digitale Proletariaat*' op verontrustende wijze de schaduwzijden zien.[49] Ook Goodman laat in recent werk op indringende wijze de donkere kanten van technologische ontwikkelingen zien.[50]
Selznick betoogt dat er vanuit theoretisch en beleidsmatig perspectief geen noodzaak is om te kiezen tussen idealisme en realisme. We dienen juist deze twee verschillende, maar complementaire, visies bij het geven van een moreel oordeel en het maken van een institutioneel ontwerp allebei te verdisconteren. In dit onderzoek is onderzocht of in de huidige digitale samenleving bijvoorbeeld *'Privacy-by-design'* bij kan dragen aan zo'n institutioneel ontwerp. Het gaat daarbij om een ontwerpprincipe voor het ontwerpproces als geheel. Naast technologische ontwerpprincipes blijven ook procedures en het beïnvloeden van menselijk gedrag van belang.
Selznick stelt het in stand houden en respecteren van de rechtsstaat[51] voorop. Tegelijkertijd is hij bekend geworden als een voorvechter van responsief recht:[52]

46. Zie 6.2.4.
47. Selznick, 1992.
48. Een bit is de kleinste eenheid van informatie.
49. Schnitzler 2015.
50. Goodman, 2015.
51. Zie over de rechtsstaat Adams 2006, Adams 2010. Adams & Witteveen 2014.
52. Nonet en Selznick, 2001 (heruitgave).

> *"The main service of responsive law is to bring 'a promise of civility' through a restructuring of social relations and a diffusion of legal authority. Civic participation and bureaucratic decentralization become the watchwords and narrow ideologies are thematized; 'law finds consensus in general aspirations rather than in specific norms of conduct.' In this way, a genuine and spontaneous 'withering away of the state' is envisaged. Such a state of affairs will be necessarily vulnerable, but the ensuing legal order will possess the capacity to be tillly representative. However, although popular participation and communal conscientiousness will be the order of the day, legality will remain irrepressible feature of this responsive society."*

Responsief recht bouwt voort op de rechtsstaat en wil de dynamiek ondersteunen. Selznick ziet responsief recht als de meest geavanceerde vorm van recht, die openstaat voor veranderingen in de samenleving. In de huidige informatiesamenleving past fijnmazige regulering via alleen 'klassieke' wetten en regels niet bij de snel veranderende, tijd- en plaatsonafhankelijke informatietechnologie.

De term responsiviteit is naast het genoemde werk van Selznick bekend geworden door het gezamenlijke werk van Nonet en Selznick in hun boek '*Law and Society in Transition. Toward responsive Law (1978)*'.[53] Zij onderscheiden drie typen van recht en rechtsvinding: '*autonomous*', '*repressive*' en '*responsive*'. Autonoom recht ontwikkelt zich volgens eigen juridische logica en doctrines. Het is de meest legalistische variant van de drie, waarbij rechtszekerheid en formele gelijkheid belangrijke waarden zijn. Dit type van recht past bij samenlevingen die door continuïteit en politieke stabiliteit worden gekenmerkt.
In een heel ander soort samenleving – autoritaire samenlevingen bijvoorbeeld – komt een ander type recht tot wasdom: repressief recht, dat effectiviteit en algemeen belang boven procedurele gerechtigheid in het individuele geval stelt. Het derde type recht, het responsieve recht, zit niet opgesloten in zichzelf en is evenmin werktuig van de machthebbers. Het is het recht dat volgens de auteurs past bij de moderne democratische samenleving. Het responsieve recht stelt zich in dienst van de leniging van maatschappelijke noden en geeft gehoor aan de maatschappelijke verwachtingen, met inachtneming van belangrijke juridische waarden, zoals proportionaliteit en rechtmatigheid.

1.5.3 Algemene hypothese

Het voorgaande normatieve kader leidt tot de volgende hypothese:

> Personen dienen er gelet op de opmars van persoonlijke gezondheidsomgevingen op te kunnen vertrouwen dat informationele zelfbeschikking, privacy en bescherming van persoonsgegevens daadwerkelijk tot uiting kunnen komen en daarmee betekenisvol zijn. Meer dan in het verleden heeft de overheid een actievere rol om de belangen van personen te beschermen die hun gezondheidsgegevens en andere persoonsgegevens moeten of willen (laten) beheren met behulp van persoonlijke gezondheidsomgevingen. In navolging van Selznick begint een dergelijke rol van de overheid met het creëren en versterken van rechten en rechtsbescherming. Ook bij de daadwerkelijke adoptie van *privacy-by-design*[54]heeft de overheid aldus een actieve rol te vervullen.

53. Nonet en Selznick, met een nieuwe introductie door Robert A. Kagan, 2001. Zie verder paragraaf 3.3.
54. De AVG spreekt over 'gegevensbescherming door ontwerp' (in de Engelse versie: '*data protection by design*') en van 'gegevensbescherming door standaardinstellingen' (in de Engelse versie: '*data protection by default*').

1.6 INTRODUCERENDE SCHETS

Uit de dissertatie van Van Beers[55] over lichamelijke zelfbeschikking in het tijdperk van biotechnologie, kan worden geleerd dat vanuit het Nederlandse gezondheidsrecht en -ethiek de nadruk is gelegd op de individuele zelfbeschikking.
In 1969 verschijnt van Van den Bergh het boekje 'Medische macht en medische ethiek', waarin hij betoogt dat de toegenomen medische macht een nieuwe medische ethiek vereist, die de grenzen van het handelen centraal stelt en oog heeft voor het perspectief van de patiënt. Het boekje van Van den Bergh betekent een keerpunt in de geschiedenis van de medische ethiek. Het markeert de opkomst van een medische ethiek die beoogt de patiënt te beschermen tegen de macht van de arts.[56] Centraal in deze benadering van ethiek staat het beginsel van respect voor autonomie: de arts dient de wensen van de patiënt in beschouwing te nemen en hier zo veel mogelijk recht aan te doen. In het bijzonder geldt dat artsen geen behandeling mogen uitvoeren wanneer dit door een wilsbekwame patiënt wordt geweigerd. Hiermee komt zelfbeschikking in de medische ethiek centraal te staan. De patiënt wordt de ruimte toegekend om zelf te beslissen over zijn eigen lichaam en leven, ongeacht de medische mogelijkheden. Als de patiënt een ingreep niet wenst mag deze niet worden toegepast, ook niet als deze ingreep vanuit medisch perspectief kans van slagen heeft. De patiënt krijgt daarbij nadrukkelijk de mogelijkheid om in de ogen van de arts 'verkeerde' beslissingen te nemen. Een illustratie hiervan in de actuele rechtspraak is de uitspraak van Rechtbank Noord-Holland op 12 mei 2017[57] over een vordering van een vader tot vervangende toestemming voor een medische behandeling van zijn 12-jarige zoon. De zoon wil geen verdere (chemo)behandeling na een operatie en radiotherapie van een medulloblastoom. De behandelend oncoloog heeft de zoon door een psychiater laten onderzoeken op zijn wilsbekwaamheid. De psychiater heeft de zoon wilsbekwaam bevonden. De behandelend oncoloog en de Stichting Jeugd- en Gezinsbeschermers hebben de keuze van de zoon gerespecteerd. De zaak kenmerkt zich door de vraag naar het recht op zelfbeschikking (recht op fysieke integriteit) van een 12-jarige. Volgens de wet is voor een ingrijpende medische handeling toestemming nodig van een 12-jarige, mits deze wilsbekwaam is. Bij wilsbekwaamheid heeft een 12-jarige ook het recht om geen toestemming te verlenen, ook bij levensbedreigende situaties.
Zelfbeschikking is als onderdeel van de revolutie in de medische ethiek een krachtig concept, maar niet absoluut. Niet alleen bij informationele, maar ook bij lichamelijke zelfbeschikking.
Hoewel zelfbeschikking in het gezondheidsrecht een centrale waarde is, erkent het recht de almacht van de persoonlijke autonomie niet. Bijvoorbeeld het verbod op de exploitatie van organen, het verbod van commercieel draagmoederschap en het verbod op reproductief kloneren. Van Beers relativeert de

55. Zie over lichamelijke zelfbeschikking het proefschrift van Van Beers, 2009.
56. In het licht van informationele zelfbeschikking is inmiddels de vraag: wie beschermt personen tegen het gebruik van gezondheidsgegevens door machtige partijen die buiten de zorgcontext met ponder andere een medisch beroepsgeheim worden verwerkt?
57. ECLI:NL:RBNHO:2017:3955.

dominantie van zelfbeschikking en pleit voor meer reflectie op het beginsel van de menselijke waardigheid.[58]

Sinds de opkomst van de informatiemaatschappij wordt het begrip zelfbeschikking niet alleen gebruikt in de context van 'lichaam en leven'[59], maar ook in de context van persoonsgegevens: informationele zelfbeschikking.[60] Daarmee is een duidelijke link gelegd met de zelfbeschikking over en controle op gezondheidsgegevens. In paragraaf 3.2 wordt nader betoogd dat menselijke waardigheid ook een belangrijk beginsel is voor informationele zelfbeschikking. Analoog aan de genoemde voorbeelden van een verbod op lichamelijke zelfbeschikking zou in lijn van Jacobs betoogd kunnen worden dat met het oog op menselijke waardigheid er ook een verbod zou moeten komen op het commercieel exploiteren van gezondheidsgegevens:

> *"In de niet-digitale wereld zijn we niet bang om bepaalde zaken te verbieden. Je eigen organen mag je niet verkopen. Dat is goedbeschouwd een vorm van betutteling en een beperking van de individuele vrijheid. Toch vinden we het verbod een vorm van beschaving, vooral omdat we niet willen dat arme mensen in een afhankelijke situatie geen andere keus zien dan hun organen te verkopen. Soms moet je mensen tegen zichzelf beschermen. Ook in de digitale wereld. Waarom zou je je organen niet mogen verkopen, maar je persoonlijke medische gegevens wel?"*[61]

Mogelijk is zo'n verbod op te nemen bij te ontwikkelen wetgeving inzake persoonlijke gezondheidsomgevingen?
In 1983 is in Duitsland het recht op informationele zelfbeschikking gedefinieerd als 'het recht van het individu om in beginsel zelf te beschikken over de openbaarmaking en het gebruik van persoonlijke gegevens'[62]. Informationele zelfbeschikking is de meest vergaande verwoording. Bestudering van 'informationele zelfbeschikking' in Duitsland leidt tot de conclusie dat het principiële recht op informationele zelfbeschikking als facet van het algemeen persoonlijkheidsrecht en recht op menselijke waardigheid mogelijk is en wenselijk binnen het Duitse rechtsstelsel, maar in de praktijk onvoldoende rechtsbescherming biedt tegen de snelle maatschappelijke en technologische ontwikkelingen. In het huidige maatschappelijke en technologische klimaat is onmogelijk vol te houden dat het individu de beschikking heeft over de op hem betrekking hebbende informatie en überhaupt in staat is daarover de beschikking te hebben. Op 27 februari 2008 velde het Duitse Bundesverfassungsgericht (BverfG) een arrest[63] dat belangrijke grenzen stelt aan het op afstand uitlezen van harde schijven ('online doorzoeken' of '*remote searches*') door politie en veiligheidsdiensten.[64]

58. Hendriks, 2010.
59. Lichamelijke integriteit in de zin van artikel 11 Grondwet.
60. Bundesverfassungsgericht (Constitutioneel Hof) 15 december 1983, BVerfGE, 65, 1 (43);, Dommering, 2010, ZonMw, 2013, RVZ 2014: https://www.raadrvs.nl/publicaties/item/het-recht-op-informationele-zelfbeschikking-in-de-zorg.
61. Jacobs, 2015.
62. Bundesverfassungsgericht (Constitutioneel Hof) 15 december 1983, BVerfGE, 65, 1 (43).
63. *Online Durchsuchung*, 1 BvR 370/07, 1 BvR 595/07.
64. http://www.vub.ac.be/LSTS/pub/Dehert/273.pdf.

Kijkend naar de ontwikkeling van 'informationele zelfbeschikking' in het Europeesrechtelijke domein wordt duidelijk dat in het kader van 'informationele zelfbeschikking in de zorg' van belang is dat de bescherming van medische gegevens valt onder een ruime uitleg van artikel 8 EVRM. Zo bepaalt het Europees Hof voor de Rechten van de Mens (EHRM) dat een medisch document in ieder geval onder de bescherming van privéleven valt. Het gaat hier om persoonlijke en gevoelige informatie. In dat geval overlappen privacy en bescherming van persoonsgegevens elkaar in grote mate. Het EHRM heeft zich uitgesproken over openbaarmaking, toegang, gebruik en het doorgeven van medische dossiers en correspondentie. Daarmee is echter niet gezegd dat het Duitse begrip van informationele zelfbeschikking hier overeenkomt met beide begrippen. In de literatuur is overtuigend beargumenteerd dat privacy en gegevensbescherming weliswaar verwant zijn, maar ook principieel verschillen.[65] Inmiddels is met het Handvest van de Grondrechten van de EU ook een internationaalrechtelijke basis voor deze splitsing voorhanden.[66]De bescherming van persoonsgegevens is versterkt en grotendeels geharmoniseerd in de AVG en de Uitvoeringswet AVG.[67]

Met betrekking tot de vraag of een recht op informationele zelfbeschikking in Nederland mogelijk en zinvol is, zijn suggesties hiertoe in het verleden herhaaldelijk afgewezen door de wetgever bij de herziening van de Grondwet in 1983 en het invoeren van de Wet bescherming persoonsgegevens (Wbp).[68] Daarbij werd gerefereerd aan de situatie in Duitsland. Relevant daarbij is dat uit de paragrafen 173 t/m 175 bij de uitspraak van het Duitse Constitutioneel Hof over informationele zelfbeschikking[69] blijkt dat het Duitse Constitutioneel Hof van mening is dat het recht op informationele zelfbeschikking geen absoluut recht kan zijn.

Een eventuele mogelijkheid voor een recht op informationele zelfbeschikking zou volgens de memorie van toelichting bij de Wbp aansluiting betekenen bij het algemeen persoonlijkheidsrecht, zoals dat in het Valkenhorst-arrest[70] is geformuleerd. Maar dit is een tamelijk uitzonderlijke zaak die weinig vervolg heeft laten zien. Het algemeen persoonlijkheidsrecht geldt in het Valkenhorst-arrest als grondslag voor grondrechten als het recht op privéleven, vrijheid van godsdienst en vrijheid van meningsuiting, en vormt daarmee de basis voor een recht op kennis over afstamming. Het Nederlandse rechtsstelsel gaat uit van een andere systematiek dan de Duitse grondwettelijke orde, waar sprake is van een sterke waardeoriëntatie en systematische formulering van allerlei onzelfstandige grondrechten als het recht op informationele zelfbeschikking. De Duitse rechter laat deze concepten open ter verdere interpretatie om daarmee tegemoet te komen aan nieuwe ontwikkelingen, maar formuleert nieuwe

65. Peter Blok, *Het recht op privacy*, diss. Tilburg, Den Haag: Boom Juridische uitgevers 2002 en Koops, 2011.
66. Zie Verdrag van Lissabon, 13 december 2007.
67. Zie de uitwerking van de AVG in paragraaf 5.3.6 en van de Uitvoeringswet AVG in paragraaf 6.2.2.
68. Zie: Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3, p. 9.
69. Bundesverfassungsgericht, 15 December 1983, BVerfGE, 65, 1 (43).
70. https://www.studytubelaw.nl/arresten/319-valkenhorst.

grondrechten als dat nodig is. De Nederlandse rechter heeft een andere taakopvatting en stelt zich bescheidener op. De formulering van een afgeleid grondrecht als het algemeen persoonlijkheidsrecht in het Valkenhorst-arrest is dan ook uitzonderlijk. Het ligt niet in de rede dat de Nederlandse rechter het algemeen persoonlijkheidsrecht verder uitwerkt in verschillende rechten, zoals het recht op informationele zelfbeschikking.

Afsluitend zijn voor deze eerste introductie van het begrip informationele zelfbeschikking de volgende punten nog van belang. Zoals eerder geconstateerd heeft het recht op informationele zelfbeschikking in Duitsland inmiddels aan waarde ingeboet en schiet het volgens sommige juridische onderzoekers tekort qua rechtsbescherming. Het is de vraag of de nadruk op informationele zelfbeschikking in het Nederlandse recht past. In het Nederlandse recht op bescherming van de persoonlijke levenssfeer is zowel een afweerrecht als een actief beschermende overheid vereist. Dit laatste is ook het geval ten aanzien van het Duitse recht op informationele zelfbeschikking, maar dat komt door de sterk waardengerichte inbedding in de Duitse Grondwet. De Nederlandse Grondwet heeft een minder sterk waardenfundament dan de Duitse Grondwet. Het Nederlandse perspectief op informatie is breder dan de focus op zelfbeschikking. Een alternatief zou zijn om de bescherming van persoonlijke informatie sterker in het Nederlandse recht te verankeren. Dat brengt de vraag op of voor de snelle informatietechnologische veranderingen en machtsverhoudingen voor de dagelijkse praktijk meer – aanvullende – responsieve regulering is gewenst, zoals in de voorgaande paragraaf geagendeerd.

1.7 OPZET VERVOLGHOOFDSTUKKEN

In het volgende hoofdstuk komen allereerst de afbakening van het onderzoek aan de orde en de te onderscheiden groepen personen waarvoor extra juridische en morele aandacht noodzakelijk is. Vervolgens worden zes ontwikkelingen onderscheiden bij informationele zelfbeschikking in de zorg.

Na hoofdstuk 2 volgt in het derde hoofdstuk het normatieve model. Het derde hoofdstuk is geschreven aan de hand van rechtsfilosofen. Het gedachtegoed van deze filosofen wordt toegepast op de nieuwe technologische en maatschappelijke ontwikkelingen uit hoofdstuk 2 in het licht van informationele zelfbeschikking. Met in het bijzonder aandacht voor de opmars van persoonlijke gezondheidsomgevingen.

Het vierde hoofdstuk gaat over de bakermat van informationele zelfbeschikking: Duitsland. Het begrip informationele zelfbeschikking met bijbehorende jurisprudentie en dogmatiek wordt uitgewerkt met betrekking tot Duitsland.
In hoofdstuk 5 volgt een uitwerking hiervan in Europa. In hoofdstuk 6 volgt de regulering in Nederland in het algemeen en de Nederlandse zorg in het bijzonder. Het zevende hoofdstuk volgt een normatieve veldverkenning van arrangementen voor rechtsbescherming als bijdrage aan de gedachten- en rechtsvorming.
Het slothoofdstuk, hoofdstuk 8, bevat de conclusies en aanbevelingen.

2. *Praktijkontwikkelingen*

2.1 INLEIDING

In dit hoofdstuk wordt het onderzoek nader ingekaderd. Dit gebeurt door allereerst de actuele thema's die spelen in relatie tot persoonlijke gezondheidsomgevingen, in zes type ontwikkelingen te clusteren. Daarnaast worden drie bij deze ontwikkelingen betrokken groepen onderscheiden. Het onderscheid wordt gemaakt omdat de te bespreken ontwikkelingen lijken te noodzaken tot extra aandacht wat betreft rechtsbescherming en positionering ten opzichte van andere betrokken partijen.

Relevant zijn allereerst de volgende zes – in overigens willekeurige volgorde benoemde – ontwikkelingen:

1. Toenemende behoefte aan en mogelijkheden voor persoonlijke gezondheidsomgevingen.
2. Toenemende mobiele gezondheidsgerelateerde diensten voor personen via smartphones.
3. Veranderende rol van de zorgaanbieders: gezamenlijke besluitvorming en specialisatie.
4. *Big data*, versmeltend[71] met andere nieuwe technologieën, zoals kunstmatige intelligentie, *Internet of Things* en *blockchain*[72].
5. Toenemende private aanbieders buiten de traditionele semi-publieke actoren in de zorg.
6. Toenemende invloed van de overheid.

Bij de bespreking van deze zes ontwikkelingen is steeds hetzelfde format gebruikt. Het begint met een algemene bespreking en vervolgt met een illustratie met een aantal toepassingen. Daarna volgt een duiding van de ontwikkeling in relatie tot het onderzoeksthema.

71. Ook wel NIBC-convergence genoemd: het samenkomen en vervloeien van vier belangrijke technologieën: nano, informatie, bio en cognitie.
72. In de kraamzorg is een proef gaande met als streven de patiënt/cliënt meer zeggenschap te geven over (veelal) haar zorggegevens en de zorgverlener af te helpen van een hoop administratieve rompslomp, Zie: https://nos.nl/artikel/2219980-meer-regie-patient-en-minder-papieren-rompslomp-in-zorg-door-blockchain.html. Zie over blockchain ook: Verhelst 2017.

Onderscheid in groepen personen waarvoor extra juridische en morele aandacht nodig is
'De patiënt' of 'de persoon' bestaat niet in de praktijk. Iedere persoon is uniek. Om toch enigszins te bepalen in welke mate een persoon (extra) zeggenschap dient te krijgen over zijn gezondheidsgegevens, worden in navolging van het Centrum voor Ethiek en Gezondheid (CEG) drie groepen personen onderscheiden voor wie extra juridische en morele aandacht noodzakelijk lijkt te zijn[73]:

1. degenen die zich zorgen maken over machtsmisbruik;
2. degenen die gegevens niet kunnen of willen 'managen';
3. degenen die actief zelf persoonsgegevens willen 'managen'.

Deze drie te onderscheiden groepen sluiten aan op de discoursenanalyse in de dissertatie van Pluut.[74] Pluut toont dat er drie verschillende discoursen van patiëntgerichte zorg zijn te onderscheiden. Elk van deze discoursen geeft een ander antwoord op de vraag in welke mate verschillende typen personen zelfbeschikking dienen te krijgen over hun gezondheidsgegevens:

– Aanhangers van het 'zorgen voor patiënten'-discours menen dat patiënten veel te kwetsbaar zijn voor informationele zelfbeschikking. Zij vinden dat die verantwoordelijkheid niet bij de patiënt gelegd moet worden en dat we daar heel voorzichtig mee moeten zijn.
– Volgens het *empowerment*-discours is het antwoord: informationele zelfbeschikking is een goede ontwikkeling, want het leidt tot betere zorg en betere kwaliteit van gegevens en dus moet je alle patiënten proberen daartoe te equiperen (zelfbeschikking, tenzij).
– In de argumentatie van het situationele discours moet informationele zelfbeschikking niet alleen per persoon maar ook per situatie (bij dezelfde persoon) verschillen (in de ene situatie kan de persoon zelf willen beschikken, in de andere niet). Responsiviteit lijkt hier het devies![75]

In paragraaf 3.3 ga ik nader in op responsieve regulering, geïnspireerd door Nonet & Selznick.[76]

Onderstaand volgt eerst een bespreking van de zes ontwikkelingen, te beginnen met de groeiende behoeften en mogelijkheden in relatie tot persoonlijke gezondheidsomgevingen.

73. Hooghiemstra, T en P. Ippel, Zeggenschap over het EPD, ethisch en juridisch perspectief, CEG/HEC, 2010.
74. Pluut, 2017.
75. In paragraaf 3.3 wordt nader ingegaan op responsieve regulering, geïnspireerd door Nonet & Selznick, 2001:17.
76. Nonet & Selznick, 2001:17.

2.2 BEHOEFTEN EN MOGELIJKHEDEN PERSOONLIJKE GEZONDHEIDSOMGEVINGEN

2.2.1 Inleiding

In hoofdstuk 1 werd gewezen op de voorspelling van Topol dat we in de toekomst een gepersonaliseerd en gedigitaliseerd profiel van onze gezondheid bij ons zullen dragen. Dit toekomstbeeld lijkt te passen in het streven van het Informatieberaad Zorg om via het programma 'MedMij' persoonlijke gezondheidsomgevingen een prominente plek te laten innemen in de Nederlandse zorg, overeenkomstig het eerdere advies 'Patiënteninformatie' van de RVZ[77]. De RVZ gaf daar de volgende redenen voor:

1. onvoldoende mogelijkheden voor de patiënt om preventie en zelfmanagementgegevens zelf (digitaal) bij te houden;
2. onvoldoende mogelijkheden voor de patiënt om zijn persoonlijk zorgnetwerk te informeren, managen en betrekken;
3. onvoldoende mogelijkheden voor de patiënt om digitaal inzicht te hebben in zijn gezondheidsgegevens.

Overigens komt er wat betreft digitale inzage vanaf juli 2020 verandering via de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). Weliswaar pas drie jaar na inwerkingtreding van de wet op 1 juli 2017, vanwege het nog niet behaalde benodigde betrouwbaarheidsniveau voor authenticatie, zal dan het elektronisch inzagerecht realiteit zijn.[78] De AVG voorziet overigens al in een elektronisch inzagerecht vanaf 25 mei 2018. Dit recht kan ook bij gaan dragen aan digitaal inzicht in gezondheidsgegevens.

2.2.2 Behoefte en mogelijkheden

De RVZ stelde in het advies Patiënteninformatie: '*De patiënt moet desgewenst regie hebben over zijn gegevens*'. In dit digitale tijdperk maken veel mensen gebruik van allerhande diensten op internet: online bankieren, online winkelen, online chatten via sociale media en online belastingaangifte doen. Ook in de zorg kunnen personen steeds meer online. Een persoonlijke gezondheidsomgeving kan personen helpen gezondheidsinformatie, preventie en zelfmanagement te integreren. Overigens is een persoonlijke gezondheidsomgeving juridisch gezien geen dossier dat valt onder de dossierplicht van de zorgaanbieder.[79] Het kan

77. RVZ 2014.
78. https://zoek.officielebekendmakingen.nl/blg-780664.pdf, door het kabinet 25 augustus 2016 gevoegd bij de Kamerstukken over het eID Debat https://www.rijksoverheid.nl/documenten/kamerstukken/2016/08/25/kamerbrief-over-impuls-eid. Op 4 november 2016 gaf de minister van VWS een reactie op het rapport naar aanleiding van Kamervragen, zie: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2016/11/04/kamerbrief-reactie-op-rapport-onderzoek-betrouwbaarheidsniveau-patientauthenticatie-bij-elektronische-gegevensuitwisseling-in-de-zorg/kamerbrief-reactie-op-rapport-onderzoek-betrouwbaarheidsniveau-patientauthenticatie-bij-elektronische-gegevensuitwisseling-in-de-zorg.pdf.
79. In de zin van artikel 454, eerste lid, boek 7 Burgerlijk Wetboek (Wet geneeskundige behandelingsovereenkomst, WGBO).

naast en in aanvulling op het wettelijk verankerde dossier van de zorgaanbieder vrijwillig worden bijgehouden door een persoon.

De behoefte van burgers aan dergelijke omgevingen lijkt zeker aanwezig. In het voor deze dissertatie uitgevoerde onderzoek van CentERdata is aan 2.730, leden van het CentERdatapanel een aantal vragen voorgelegd over informationele zelfbeschikking in de zorg, waarvan 1,925 de vragenlijst volledig invulden, oftewel met een respons van 71%.[80] Het onderzoek pretendeert representatief te zijn voor de hedendaagse samenleving.

Ten aanzien van persoonlijk gezondheidsomgevingen zijn de volgende vragen gesteld:

1. Zou u willen dat het mogelijk was om via het internet eenvoudig een overzicht te kunnen inzien van de gezondheidsgegevens die over u staan geregistreerd?
2. Toelichting: waarom men wel zou willen dat het mogelijk was om via het internet eenvoudig een overzicht te kunnen inzien van de gezondheidsgegevens ?
3. Toelichting: waarom men niet zou willen dat het mogelijk was om via het internet eenvoudig een overzicht te kunnen inzien van de gezondheidsgegevens
4. Zou u de mogelijkheid willen hebben om uw gezondheidsgegevens zelf te controleren en beheren?
5. Zou u het een goed idee vinden als een ICT bedrijf zorg draagt voor de opslag van uw gezondheidsgegevens?
6. Toelichting: waarom men het geen goed idee vindt als een ICT bedrijf zorg draagt voor de opslag van medische gegevens?
7. Een persoonlijk gezondheidsdossier kan door verschillende instanties worden beheerd, maar ook door u zelf. Waar zou uw voorkeur naar uitgaan?

De meest opvallende algemene uitkomsten van dit onderzoek zijn:

– "Ruim 60% van de geënquêteerde Nederlanders wil een persoonlijke gezondheidsomgeving, hoewel ze niet precies weten wat het is.[81]
– De meerderheid van deze groep (53%) wil hun persoonlijke gezondheidsomgeving laten beheren door een zorgaanbieder.
– 21% kiest ervoor om persoonlijke gezondheidgegevens in eigen beheer te houden.
– 21% vertrouwt zijn persoonlijke gezondheidsomgeving toe aan grote internationale ICT-bedrijven zoals Microsoft, Apple en Google.[82]

80. Dit onderzoek is zowel uitgevoerd voor het advies Patiënteninformatie (2014) van de RVZ als voor deze dissertatie.
81. Aangezien men bij dit opinieonderzoek nog geen concrete ervaring had met een persoonlijke gezondheidsomgeving is het van belang in de praktijk te bezien in hoeverre men feitelijk van persoonlijke gezondheidsomgevingen gebruik gaat maken.
82. Dat neemt niet weg dat deze bedrijven fors investeren in persoonlijke gezondheidsomgevingen, zie bijvoorbeeld https://www.bnr.nl/radio/bnr-internet-vandaag/10324744/apple-wil-jouw-medisch-dossier-in-de-iphone.

– Voor 62% van de mensen die een persoonlijke gezondheidsomgeving willen, is bescherming van persoonsgegevens een belangrijk aandachtspunt."

Verder blijkt uit de enquête een significant verschil tussen mannen en vrouwen wat betreft het aandeel dat aangeeft dat de overheid een persoonlijke gezondheidsomgeving voor hen zou moeten bijhouden: "10% van de mannen kiest voor deze optie, tegenover 4% van de vrouwen. Opvallend is hier dat wanneer mensen met een medische fout te maken hebben gehad 12% kiest voor de overheid. Voor de mensen die hier niet mee te maken hebben gehad, geldt dat 5% voor de overheid kiest."
Meer gedetailleerde informatie over het onderzoek dat ik voor deze dissertatie en het advies Patiënteninformatie van de RVZ door CentERdata liet uitvoeren is digitaal te vinden via: https://www.centerdata.nl/sites/default/files/bestanden/achtergrondstudie_recht_op_informationele_zelfbeschikking_in_de_zorg.pdf
Het onderzoek toont geen significante verschillen naar opleiding en inkomen, maar wel naar leeftijd. De relevantie van leeftijd kwam al eerder uit onderzoek naar voren. Zo blijkt uit het proefschrift van Steijn[83] dat jongeren en ouderen vanuit andere generationele termen tegen informationele zelfbeschikking aan te kijken. Jongeren hebben andere behoeften, ander gedrag en andere zorgen dan ouderen. Ouderen krijgen door levenservaring een breder beeld. De informationele kant van zelfbeschikking zien veel jongeren nog niet. Uit het onderzoek van Steijn blijkt dat jongeren nu nog privacy met vrienden willen. Juist Facebook geeft dan bijvoorbeeld privacy, weg van ouders, dichtbij vrienden. Naarmate steeds meer ouders op Facebook gaan, wordt Facebook minder populair onder jongeren. In andere woorden het gaat bij jongeren meer om relationele privacy en om privacy binnen de context van vrienden. Wat betreft het onderscheid tussen ouderen en jongeren in relatie tot een persoonlijke gezondheidsomgeving, komen uit de voor deze dissertatie uitgevoerde survey nog de volgende observaties naar voren:

– Jongeren willen in meerderheid slechts informationele zelfbeschikking over medische gegevens als dat op een veilige wijze valt te realiseren.
– Ouderen stellen vooral als voorwaarde dat zij willen kunnen zien en controleren wat er met hun gegevens gebeurt.
– Jongvolwassenen (25-34 jaar) zijn bij een persoonlijke gezondheidsomgeving het meest bezorgd over de bescherming van persoonsgegevens.

Ook uit internationaal onderzoek blijkt de behoefte bij personen aan informationele zelfbeschikking. Van de deelnemers aan een onderzoek uit 2015 onder 28.000 Europeanen had slechts 15% het gevoel controle te hebben over zijn persoonlijke data.[84]

83. Steijn, 2014.
84. European Commission, Eurobarometer (2015). http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf.

In een poll onder 24.143 internetgebruikers uit 24 landen geeft 79% van de ondervraagden aan zich zorgen te maken over het gebrek aan online zelfbeschikking.[85]
De behoefte aan informationele zelfbeschikking blijkt – in het bijzonder voor Nederlanders en Duitsers – ook uit een onderzoek in januari 2017 van het 'Gesellschaft für Kommunikationsforschung (GfK)'.[86] GfK interviewde in de zomer van 2016 online meer dan 22.000 consumenten van 15 jaar en ouder in 17 landen. 27% van alle internetgebruikers in deze landen waren in hoge mate bereid hun persoonlijke data te delen voor een voordeeltje of kostenreductie, terwijl 19% dit expliciet niet wilde. Het bleek dat internetgebruikers uit Nederland en Duitsland het minst bereid zijn persoonlijke data te delen voor een voordeeltje (12%). Chinezen het meest (38%).

Kijkend naar de ontwikkelingen in Nederland zijn de volgende voorbeelden illustratief voor de stappen die worden gezet in het aanbieden van persoonlijke gezondheidsomgevingen.

Programma MedMij
Het MedMij-programma is een programma van het Informatieberaad Zorg.[87] Het Informatieberaad Zorg bestaat uit uit de volgende deelnemers:

- ActiZ (organisatie voor zorgondernemers in de care-sector);
- Federatie Medisch Specialisten (FMS);
- Geestelijke Gezondheidszorg (GGZ) Nederland;
- InEen (organisaties in de Eerste Lijn);
- Koninklijk Nederlands Genootschap voor Fysiotherapie (KNGF);
- Koninklijke Nederlandse Maatschappij ter bevordering der Pharmacie (KNMP);
- Landelijke Huisartsen Vereniging (LHV);
- Ministerie van VWS;
- Nederlandse Federatie van Universitair Medische Centra (NFU);
- Nederlands Huisartsen Genootschap (NHG);
- Nederlandse Vereniging van Ziekenhuizen (NVZ);
- Patiëntenfederatie Nederland;
- Vereniging Gehandicaptenzorg Nederland (VGN);
- Vereniging van Nederlandse Gemeenten (VNG);
- Verpleegkundigen & Verzorgenden Nederland.

De Patiëntenfederatie Nederland coördineert het programma en vormt samen met Nictiz en het ministerie van VWS het uitvoerende programmateam. De stuurgroep, met daarin leden van het Informatieberaad Zorg, stuurt het programmateam aan.

85. Centre for International governance Innovation & Ipsos, '2016 CGI-Ipsos Global Survey on Internet Security and Trust'(2016). https://www.cigionline.org/internet-survey-2016.
86. Gesellschaft für Kommunikationsforschung, 2017, zie: https://www.gfk.com/fileadmin/user_upload/country_one_pager/NL/images/Global-GfK_onderzoek_-_delen_van_persoonlijke_data.pdf.
87. https://www.informatieberaadzorg.nl/over-het-informatieberaad/programma%E2%80%99s/medmij

MedMij streeft ernaar dat iedereen die dat wil, kan beschikken over zijn gezondheidsgegevens in één persoonlijke gezondheidsomgeving. Het MedMij-afsprakenstelsel bevat afspraken waaraan deelnemers aan het afsprakenstelsel MedMij moeten voldoen om gegevens uit te mogen wisselen via MedMij.

Inhoudelijke functionaliteiten zijn optioneel en zullen per persoon verschillen op basis van de persoonlijke behoefte en situatie. Individuen moeten daarbij kunnen kiezen voor één persoonlijke gezondheidsomgeving en niet worden gedwongen meerdere omgevingen bij te houden. Leveranciers van persoonlijke gezondheidsomgevingen gebruiken informatie uit achterliggende systemen van zorgaanbieders en kunnen daar functionaliteit aan toevoegen. Ook zullen er aanbieders van een afzonderlijke functionaliteit zijn die via het MedMij-afsprakenstelsel gegevens kunnen uitwisselen.

Voorbeelden van werkzame persoonlijke omgevingen in Nederland
Patiëntenfederatie Nederland heeft 9 maart 2018 op digitalezorggids.nl een lijst van dertien persoonlijke gezondheidsomgevingen gepubliceerd waar zorggebruikers nu al mee aan de slag kunnen.[88] Het gaat om: 1. Digitaal zorgdossier; 2. Gezondheidsmeter; 3. E-consult; 4. HealthPortal; 5. Ivido; 6. MijnZorgnet; 7. My Karify; 8. Patiënt1; 9. Patients Know Best; 10. PAZIO; 11. Selfcare; 12. Zodos; 13. Zorgdoc.

Waarschijnlijk wordt het overzicht binnenkort uitgebreid met meer persoonlijke gezondheidsomgevingen. De persoonlijke gezondheidsomgevingen zijn allemaal nog in ontwikkeling. Ze hebben functionaliteiten als 'online je medicatieoverzicht bekijken', 'een e-consult houden of 'het invoeren van zelfmeetgegevens'. De echt uitgebreide persoonlijke gezondheidsomgevingen waarmee de zorggebruiker toegang heeft tot de eigen gezondheidsgegevens en ze van daaruit veilig en vertrouwd kan verzamelen, delen en beheren, komen later in het jaar 2018 op de markt. De door Digitale Zorggids gepubliceerde persoonlijke gezondheidsomgevingen zijn allemaal met MedMij in gesprek om mogelijk te voldoen aan de kwalificatie-eisen zoals deze zijn opgesteld in het MedMij Afsprakenstelsel.

Naast de dertien persoonlijke gezondheidsomgevingen die in gesprek zijn met MedMij zijn er natuurlijk ook voorbeelden van persoonlijke gezondheidsomgevingen van grote internationale technologiebedrijven. Voorbeelden daarvan zijn:

- HealthVault van Microsoft[89];
- Gezondheidsapp van Apple, draaiend op het Apple platform Health Kit[90];
- Gezondheidsapps eCareCompanion en eCareCoordinator, draaiend op het platform HealthSuite van Philips[91];

88. https://www.digitalezorggids.nl/digitale-dienst/persoonlijk gezondheidsomgeving/producten?theme_products-page=1.
89. https://www.healthvault.com/nl/nl.
90. http://www.iculture.nl/dossiers/gezondheid-healthkit/.
91. http://www.philips.nl/healthcare/innovatie/healthsuite-digital-platform.

Qiy Afsprakenstelsel
Waar MedMij zicht richt op afspraken voor persoonlijke gezondheidsomgevingen, is het afsprakenstelsel Qiy[92] (uitgesproken als 'key') een breder beoogde applicatie, namelijk gericht op digitale zelfbeschikking in algemene zin. Het Qiy Afsprakenstelsel kan ook voor persoonlijke gezondheidsomgevingen relevant zijn.
Daarmee is Qiy een tweede voorbeeld van een afsprakenstelsel om persoonlijke gezondheidsomgevingen te voorzien van een afsprakenstelsel dat kan bijdragen aan vertrouwen en informationele zelfbeschikking. Personen zijn volgens Qiy '*in control*' over hun data als zij als het ware het centrum zijn van hun eigen netwerk. De implementatie van dat denken is technisch vertaald in een trustlaag bovenop het bestaande internet, het *Qiy Trust Framework* genaamd. Uitgangspunten zijn '*privacy & security-by-design*' en '*by default*'. De stichting beheert een afsprakenstelsel dat vergelijkbaar is met de afsprakenstelsels die ten grondslag liggen aan GSM en aan creditcardtransacties. Dit soort afsprakenstelsels is onafhankelijk, schaalbaar en interoperabel en kent spelregels op organisatorisch, juridisch en technisch vlak.
Op basis van het Qiy Afsprakenstelsel krijgen individuen toegang tot hun data, hun persoonsgegevens, zoals deze worden verwerkt door deelnemende organisaties. Vervolgens worden zij in staat gesteld deze gegevens vanuit de bron naar eigen inzicht geheel of gedeeltelijk via het Qiy Trust Framework te routeren naar deelnemende organisaties van hun keuze. Dit kan geaggregeerd of nadat personen deze gegevens zelf hebben geanalyseerd met behulp van een kunstmatig intelligente applicatie.
Een *Qiy Node* valt ook onder de eerdergenoemde definitie van een persoonlijke gezondheidsomgeving. Het hoeft immers niet per se een digitale kluis te zijn. Met een Qiy Node heeft een betrokkene op elk gewenst moment op een – volgens Qiy – veilige en beveiligde manier, toegang tot zijn persoonsgegevens en kan hij die vervolgens onder eigen regie doorsturen naar derden van zijn keuze of ertoe besluiten zijn gegevens uit verschillende bronnen zelf te analyseren met een kunstmatig intelligente applicatie, om de uitkomsten daarvan vervolgens al dan niet met derden te delen.
De routering van persoonsgegevens geschiedt op die manier onder regie van de persoon. De deelnemende organisaties moeten zich houden aan de regels van het afsprakenstelsel. Het Qiy Afsprakenstelsel bestaat uit drie lagen: technisch, organisatorisch en juridisch. Een van de eisen is dat organisaties die gebruikmaken van het Qiy Afsprakenstelsel de Algemene Voorwaarden van de persoon voor de verwerking van zijn persoonsgegevens dienen te accepteren. De stichting zorgt er volgens Qiy voor dat de regels van het Qiy Afsprakenstelsel in overeenstemming zijn met de eisen die de AVG stelt.

2.2.3 Eerste bevinding: toenemende behoeften & mogelijkheden

De behoefte en mogelijkheden om gebruik te maken van persoonlijke gezondheidsomgevingen nemen toe. Hoewel deze ontwikkeling nog in de

92. De Qiy Foundation is een onafhankelijke en non-profit stichting die een beweging in gang gezet heeft vanuit haar missie: 'Digitale Zelfbeschikking voor iedereen!'.

kinderschoenen staat, kan het snel gaan. Zoals ook de opkomst van de smartphones snel is gegaan. Dit vergt anticiperen op zowel de kansen als de bedreigingen. Om dat mogelijk te maken, is in deze dissertatie in kaart gebracht welke behoeften er zijn onder de bevolking omtrent het faciliteren van de rechten van een persoon waar het gegevens over zijn of haar gezondheid betreft[93]. Ook al kunnen veel mensen zich hierbij nog geen concrete voorstelling maken. Uit onderzoek[94] komt naar voren dat personen verschillende behoeften hebben. De meeste personen maken zich zorgen over de effecten van digitale ontwikkelingen op de bescherming van gegevens over hun gezondheid. Zij hebben verschillende wensen en vertrouwen niet iedere partij in dezelfde mate hun gezondheidsgegevens toe. Bij het in gebruik nemen van persoonlijke gezondheidsomgevingen is het zaak om op een effectieve manier rekening te houden met de zorgen en wensen van – verschillende soorten – personen.

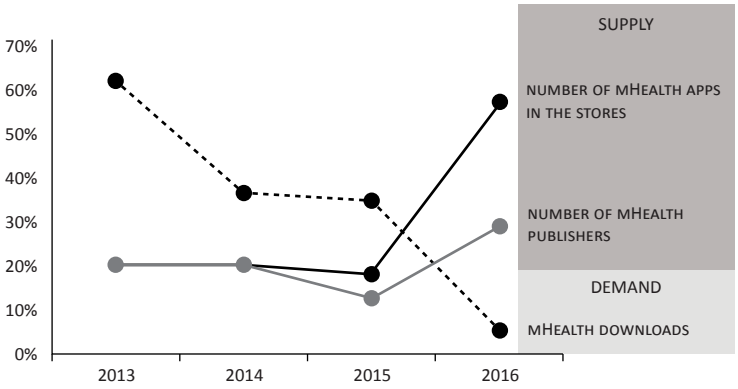
2.3 MOBIELE GEZONDHEID

2.3.1 Inleiding

Evans laat in zijn presentatie van december 2016 zien dat '*mobile is eating the world*'.[95] Wereldwijd zijn er op dit moment 2,5 miljard gebruikers van smartphones en dat stijgt snel naar 5 miljard, terwijl het aantal pc's blijft steken op ruim 1 miljard. De omzet van Google, Apple, Facebook en Amazon is inmiddels drie keer zo groot als Microsoft en Intel. De groei van het aantal pc's en laptops heeft inmiddels plaatsgemaakt voor de groei van mobiele apparaten en appsin een omvang die een veelvoud is van wat we bij de pc's en laptops hebben gezien. Smartphones zijn zonder enige twijfel de succesvolste consumententechnologie van de afgelopen tien jaar. We gebruiken de smartphone ook steeds meer: meer minuten per dag, meer datagebruik.[96] Als gevolg hiervan neemt ook *mobile Health* of *mHealth* toe.
Via een smartphone kunnen medische meetwaarden worden meegegeven en via apps kunnen persoonlijke gezondheidsomgevingen worden bijgehouden, zoals we in de vorige paragraaf al zagen.
De Duitse marktonderzoekers van *research2guidance* gaven in 2016 voor de zesde keer hun jaarlijkse onderzoek uit naar trends op de wereldwijde markt voor gezondheidsapps. Voor dit onderzoek vulden meer dan 2600 ontwikkelaars en andere betrokkenen een online vragenlijst in. Meer dan de helft daarvan komt uit Europa.
In die zes jaar is de globale markt voor smartphones geëxplodeerd, en het aanbod van mHealth-apps volgde die ontwikkeling. Sinds 2016 is er voor het eerst een afname in de groei van het aanbod. Ondanks de teruggang in groei nam het

93. Bijvoorbeeld het voor deze dissertatie uitgevoerde onderzoek van CentERdata, waarbij aan de leden van het CentERdata-panel een aantal vragen over behoeften en mogelijkheden is voorgelegd over informationele zelfbeschikking in de zorg, naast de aangehaalde secundaire onderzoeken en praktijkvoorbeelden.
94. Hooghiemstra & Ippel, 2011.
95. http://ben-evans.com/benedictevans/2016/12/8/mobile-is-eating-the-world.
96. '2 billion Consumers Worldwide tot get Smart(phones) by 2016' (2014). http: www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694.

totale aanbod in de diverse *app stores* toe tot naar schatting 350.000 gezondheid-apps in februari 2018[97].
Volgens Chavannes, hoogleraar *e-health*-toepassingen in Leiden, weten we niet in hoeverre die gezondheidsapps betrouwbaar en onafhankelijk zijn. Sinds maart 2018 heeft Leiden daarom een Nationaal *eHealth Living Lab* (NeLL), een instelling die digitale middelen om ziekten te monitoren en gezondheid te verbeteren, onderzoekt. In het *lab* kunnen digitale gezondheidsmiddelen zoals apps, sensoren, wearables en robots getest worden door patiënten, en ook door artsen, onderzoekers en ICT'ers. Volgens Chavannes is het grootste deel van de gezondheidsapps nooit goed onderzocht. Met NeLL wil hij het kaf van het koren scheiden. Een groep van ongeveer 20.000 studenten test en beoordeelt de apps. Niet alleen of de informatie daarin klopt, maar ook of die begrijpelijk is.



Aanbod groeit sneller dan vraag – Bron: research2guidance mHealthApp Developer Economics study 2016

Topol voorspelt in zijn boek *'The Patiënt Will see you now'* dat de smartphone de controle over gezondheidsgegevens direct bij personen brengt. In de volgende paragrafen zullen we bezien in hoeverre personen zelf controle krijgen over de gezondheidsgegevens en in hoeverre het (on)gewenst is dat zorgaanbieders, bedrijven en overheden hierbij ook een rol kunnen spelen.

2.3.2 Praktijkvoorbeelden

In hoofdstuk 1 toonde Topol een reeks toepassingen. Een *app*, bijvoorbeeld, om via de microfoon onze ademhaling digitaal te analyseren of onze longfuncties te meten. Een 'elektronische neus', om via een ademhalingsanalyse bepaalde types van kanker op te sporen. Of een miniatuurlaboratorium dat als aanhangsel van een smartphone razendsnel zeer kleine hoeveelheden bloed, urine of speeksel kan analyseren.

97. https://nos.nl/nieuwsuur/artikel/2219489-van-de-350-000-gezondheidsapps-is-maar-een-deel-betrouwbaar.html.

Enkele andere voorbeelden[98]:

- In Balanz, een app voor hulp bij hyperventilatie, angst en stress.
- Mensen met chronische pijnklachten kunnen op hun telefoon of tablet een pijndagboek bijhouden via een app waarmee ze het pijnverloop op de minuut kunnen volgen.
- *Mood* Meter. Hiermee kunnen gebruikers hun emoties monitoren om zo gevoelspatronen te ontdekken die hun leven beheersen. Door het aanleren van bepaalde technieken die de app voorschrijft, kan de gebruiker bewuster met zijn gevoelens omgaan.
- Ook voor chronische aandoeningen zoals COPD, hart- en vaatziekten of diabetes zijn er apps op de markt. De meeste daarvan zijn te downloaden via de App Store op de smartphone of via internet.
- De *uGrow-app* voor ouderschap, waarmee ouders onder meer gegevens delen met – en gepersonaliseerd advies ontvangen van – beroepsbeoefenaren in de gezondheidszorg. Met hulp van *American Well* biedt de app een beveiligde, ondemand videoverbinding met een kinderarts, medische arts of specialist in de geestelijke gezondheidszorg, online of via de mobiele telefoon, 24 uur per dag, 7 dagen per week.

2.3.3 Eerste bevinding: smartphone faciliteert groei mobiele zorg

Het enorme commerciële succes van de smartphone heeft de persoonlijke gezondheidsomgeving letterlijk binnen handbereik gebracht. Er bestaan reeds vele *apps* die het bijhouden en beïnvloeden van de eigen gezondheid mogelijk maken. Het bestaan van de mogelijkheid hiertoe wil echter nog niet zeggen dat dit type *apps* daadwerkelijk succesvol is. Welke *apps* uiteindelijk hun populariteit weten te behouden en effectief zullen blijken, is niet te voorspellen. Het feit dat er in februari 2018 wereldwijd naar schatting al 350.000 gezondheidsapps waren, in allerlei soorten en van diverse kwaliteit, geeft aan dat deze ontwikkeling maatschappelijk relevant is. NeLLte Leiden gaat de betrouwbaarheid en onafhankelijkheid van alle gezondheidsapps toetsen.

2.4 VERANDERENDE ROL ZORGAANBIEDERS

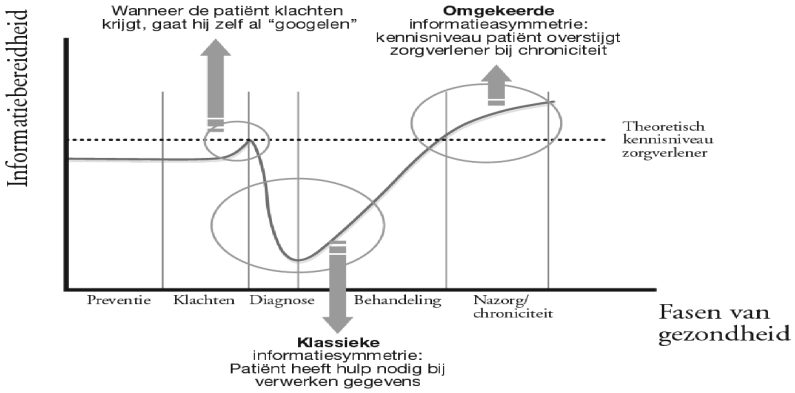
2.4.1 Inleiding

Zoals in paragraaf 2.2.2 beschreven, bleek uit het voor deze dissertatie en de RVZ uitgevoerde onderzoek van CentERdata dat de meerderheid van de geënquêteerde Nederlanders (53%) hun persoonlijke gezondheidsomgeving wil laten beheren door een zorgaanbieder, bij voorkeur de huisarts.[99]
Volgens het een jaar eerder uitgebracht advies van dezelfde RVZ, 'De participerende patiënt'[100], willen patiënten en zorgverleners meer 'gezamenlijke besluit-

98. https://www.raadrvs.nl/uploads/docs/Artikel_HP_De_Tijd_-_Big_doctor_is_watching_you..pdf en https://www.ed.nl/philips/philips-gaat-samenwerking-aan-met-american-well~ad5940b3/.
99. Dit onderzoek is zowel uitgevoerd voor het advies Patiënteninformatie (2014) van de RVZ als voor deze dissertatie.
100. RVZ 2013.

vorming en gedeelde uitvoering' om de kwaliteit van zorg en de effectiviteit te bevorderen.
Nieuw in dit advies was onder andere het pleidooi voor een recht op een Individueel Zorgplan en de beweging van 'patiënt centraal' naar 'de relatie patiënt-zorgverlener centraal'.

Uit onderzoek[101] blijkt dat voor de relatie patiënt-zorgaanbieder het idee van '*shared decision-making*' een vruchtbaar uitgangspunt is: de patiënt wordt serieus genomen en betrokken bij de behandeling. De zorgverlener steunt en begeleidt hem.
Uit een in 2010 door het HEC voor de RVZ uitgevoerd onderzoek bleek eveneens dat patiënten begeleiding en hulp nodig hebben van hulpverleners, familieleden en vrienden bij het uitoefenen van informationele zelfbeschikking, met name in spanningsvolle situaties rond (ernstige) diagnoses en bij mensen die niet goed in staat zijn over zichzelf te beschikken.[102]



Bron: RVZ, 2010

Toelichting figuur: Patiënten hebben begeleiding en hulp nodig van hulpverleners, familieleden en vrienden bij het uitoefenen van informationele zelfbeschikking, met name in spanningsvolle situaties rond (ernstige) diagnoses.

Ook in de geneeskundige literatuur wordt *shared decision making* vaak gezien als een stap op weg richting meer zelfbeschikking voor de patiënt en een evenwichtigere zorgverlener-patiëntrelatie.[103] Al het genoemde onderzoek en de bijbehorende literatuur gaat niet uit van een ideaal van volledige informationele zelfbeschikking voor patiënten, maar van een verandering in de rol van zorgverleners naar die van begeleider van personen.[104] Belangrijk daarbij is de benadering van de persoon vanuit een biopsychosociaal perspectief en het delen van macht en verantwoordelijkheid in de zorgrelatie.[105] Het gaat er nadrukkelijk om mensen in staat te stellen de zorg voor hun gezondheid zo

101. Zie NIVEL, 2011.
102. HEC, 2010.
103. Zie Vermunt 2017, Elwin, 2014, Stiggelbout, 2012 en Makoul, 2006.
104. Zie Pluut, 2017, Discours 1 van patientgerichtheid hoofdstuk 1, pagina 17 en hoofdstuk 5.
105. Duggan, 2016.

veel mogelijk zelf vorm te geven. Voor een deel van de mensen betekent dit mogelijkheden bieden om de regie te voeren over hun eigen zorg. Iedere persoon heeft daarin echter andere voorkeuren en vooral ook mogelijkheden. Deze kunnen per situatie verschillen. Zorg hangt ook samen met kwetsbaarheid en kwetsbare mensen. Persoonsgerichte zorg betekent rekening houden met deze verschillen. Al is er dan nog steeds de keuze: kwetsbaarheid accepteren of mensen weerbaar maken. Dat is een kernstrijdpunt in discussies over de rol van de zorgverlener.
Overigens heeft de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) laten zien dat informationele zelfbeschikking problematisch kan zijn.[106] Voor 'de grote meerderheid van de Nederlanders' zijn extra keuzes eerder een probleem dan een oplossing, aldus de WRR. 'Zelfredzaamheid' is niet alleen een probleem voor mensen met een laag IQ. Ook personen met een hoge opleiding en een goede maatschappelijke positie zijn soms minder zelfredzaam dan de overheid verwacht, zeker als het leven tegenzit, bijvoorbeeld bij scheiding, ontslag of faillissement. Het gaat in het contact met de overheid namelijk niet alleen om 'denkvermogen', maar ook om 'doenvermogen', schrijft de WRR. 'Het vermogen om in actie te komen, om het hoofd voldoende koel te houden, en om vast te houden aan goede voornemens.' Voor nieuwe ontwikkelingen, zoals persoonlijke gezondheidsomgevingen, zijn daarom aanvullende randvoorwaarden noodzakelijk om personen te beschermen: niet alleen informeren, maar ook sturen en ondersteunen.

In hoofdstuk 1 zagen we dat volgens Topol de smartphone de controle over gezondheidsgegevens direct bij personen brengt. Dat een persoon bijvoorbeeld zelf al een Elektrocardiagram (ECG)[107] kan maken met zijn smartphone en daarbij ook nog eens een interpretatie krijgt van een computer, waarna de dokter kan nagaan of de computer gelijk heeft. Dat betekent volgens Topol dat de rol van de zorgaanbieder in en rond de behandeling drastisch verandert en ook de rol van personen. Zij krijgen met de smartphone en andere apparaten immers voor het eerst een instrument in handen om zelf hun gezondheid te monitoren en informatie over hun gezondheid te beheren. De smartphone geeft hen toegang tot gezondheidsinformatie. Personen kunnen dan zelf bepalen of ze deze gegevens willen delen met hun arts of andere zorgverleners.
In het advies Consumenten eHealth[108] heeft de RVZ deze nieuwe eHealth-ontwikkelingen onder de aandacht gebracht. Onder consumenten-eHealth verstaat de RVZ:

> *"Direct op de markt zonder tussenkomst van zorgverleners aan de consument aangeboden informatie- en communicatietechnologie, die beoogt de gezondheid van gebruikers te ondersteunen of verbeteren."*

Net als Topol verwacht de RVZ dat deze ontwikkeling de rol van zowel de zorgaanbieders als personen ingrijpend zal veranderen. De RVZ verwacht daarnaast ook een gedeeltelijke vervlechting van consumenten-eHealth en reguliere zorg.

106. WRR, 2017.
107. Hartfilmpje.
108. RVZ 2015.

Op onderdelen zou consumenten-eHealth reguliere zorg kunnen vervangen en zorg zal steeds meer tijd- en plaatsonafhankelijk worden.

In de praktijk verwacht de RVZ dat in ieder geval bij ingewikkelde geneeskundige behandelingen er sprake zal zijn van een samenspel tussen zorgverlener en patiënt. Zorgverleners zullen zich naar verwachting van de RVZ meer gaan toeleggen op complexe diagnostiek en gezamenlijke besluitvorming, waarin persoonlijke afwegingen belangrijk zijn. Daarnaast houden zij een belangrijke rol in de zorg voor kwetsbare personen.
Gezamenlijke besluitvorming met behulp van eHealth vindt steeds meer plaats via patiëntenportalen bij zorgaanbieders. Hieronder enkele praktijkvoorbeelden.

2.4.2 Praktijkvoorbeelden

PAZIO
PAZIO[109] biedt een eHealth-portaal voor zorg en welzijn dat zorgverleners en hun eHealth-diensten samenvoegt. Hiermee krijgen zorggebruikers via één digitale voordeur toegang tot hun online zorg- en welzijnsdiensten.
Patiënten en cliënten loggen één keer in met DigiD en sms[110] en hebben toegang tot zorgdiensten, maar ook tot die van andere zorgverleners waar zij onder behandeling zijn, van huisarts tot fysiotherapeut en van buurtteam tot het ziekenhuis. Het betreft een overkoepelend patiëntenportaal: discipline- en lijnoverstijgende zorg samengevoegd achter één inlog.

PAZIO is slechts een van de patiëntenportalen in Nederland. Nictiz heeft in het najaar van 2017 de op dat moment bestaande patiëntportalen bij ziekenhuizen met elkaar vergeleken. Het volledige overzicht is te zien via: www.hoeonlineisjouwziekenhuis.nl. Het overzicht toont dat bij 34 ziekenhuizen online de gezondheidsgegevens zijn in te zien. Ook de functionaliteiten die de patiëntenportalen van ziekenhuizen beschikbaar stellen, zijn zichtbaar. Eveneens is zichtbaar of je als patiënt goed geïnformeerd wordt over de mogelijkheden. 22 ziekenhuizen bieden bijvoorbeeld inzage in medicatieoverzicht en 31 in onderzoeksgegevens zoals laboratoriumresultaten. Onderdeel van de website is de overzichtskaart waarin iemand kan zien of het eigen ziekenhuis een portaal met online inzage heeft, en zo ja wat er dan allemaal op dat portaal te vinden is. Door het Versnellingsprogramma Informatie-uitwisseling Patiënt & Professional (VIPP) zullen waarschijnlijk binnen een korte tijd veel meer ziekenhuizen en instellingen patiëntenportalen hebben. In de miljoenennota voor het begrotingsjaar 2016 is een bedrag van 105 miljoen euro voor het versnellingsprogramma opgenomen dat loopt tot eind 2019. Zie: https://www.vippprogramma.nl/over-vipp. Het hebben van een portaal leidt overigens niet automatisch tot betere zorg.

109. In dit Youtube-filmpje is uiteengezet wat PAZIO doet: https://www.youtube.com/watch?v=uarLq0YiH98.
110. Met deze tweestapsverificatie voldoet PAZIO aan de eisen die de AP op dat moment aan patiëntportalen stelde. Op 19 december 2016 werd bekend dat de AP bij veel patientportalen heeft waargenomen dat zij niet aan deze eis voldoen, zie: http://nos.nl/artikel/2149209-gegevens-in-patientenportaal-niet-veilig.html.

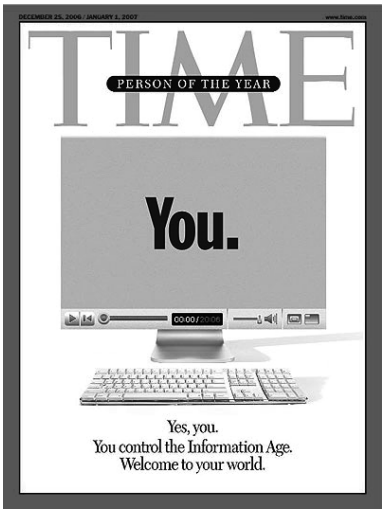
2.4.3 Eerste bevinding: zorgverlener wordt begeleider

De rol van zorgaanbieders – met inbegrip van individuele zorgverleners – verandert doordat steeds meer mensen zelf over hun gezondheidsgegevens en bijbehorende medische informatie kunnen beschikken. Voor hen verandert de rol van zorgverlener in die van begeleider. Er kan dan sprake zijn van *shared decision making*. De zorgverlener blijft verantwoordelijk voor het bijhouden van gegevens over een persoon op grond van de dossierplicht. Bezien vanuit de markt voor persoonlijke gezondheidsomgevingen kunnen zowel de zorgverlener als de persoon gebruiker zijn van een elektronische dienst. Nog niet vast staat in hoeverre een persoon daadwerkelijk gebruik zou kunnen of willen maken van gezondheidsgegevens over zichzelf.

2.5 *BIG DATA* IN DE ZORG

2.5.1 Inleiding

In de voorgaande paragrafen kwamen smartphones, persoonlijke gezondheidsomgevingen en patiëntenportalen al aan bod. Al deze gegevensdragers zijn met elkaar verbonden en het verwerken van gegevens, zowel persoonsgegevens als andere gegevens, is ook in de zorg in korte tijd toegenomen.



In 2006 werd 'You' nog gekozen als Time[111] magazine's *Person of the Year*. Deze onderscheiding was volgens Time een erkenning van de miljoenen mensen die anoniem bijdragen aan door individuele gebruikers gegenereerde inhoud op sociale media.[112]

111. Time 25 november 2006.
112. Zoals Wikipedia, YouTube, MySpace en Facebook.

In 2006 beschouwde Time het nog als een positieve verworvenheid van het open internet dat miljoenen gebruikers bijdragen aan content op social media. Inmiddels loggen miljoenen gebruikers in met hun smartphones en produceren daarmee *big data* op een ongekende schaal, met zowel kansen als bedreigingen, ook in de zorg.

Volgens Van den Hoven bevinden we ons in een big-datasamenleving[113], waarbij nieuwe technologieën het mogelijk maken om steeds grotere datasets te verzamelen, op te slaan en te koppelen. Deze datasets maken van personen niet alleen een gebruiker van een big-datatechnologie, zoals de Time in 2006 idealiseerde, maar ook een databron.
Inmiddels moeten wij moeite doen om geen informatie te verwerken. In de AVG staat als reactie op deze ontwikkeling 'het recht op vergetelheid' centraal, hoewel dit slechts ten dele een nieuw recht is ten opzichte van de Wbp.[114] Ook stelt de AVG in artikel 22 voorwaarden aan profilering met behulp van *big data*. Op basis van profilering mogen geen besluiten met rechtsgevolg genomen worden zonder menselijke tussenkomst en profilering mag ook niet zonder toestemming van de betrokken persoon. Working Party (WP) 29 van de gezamenlijke toezichthouders voor gegevensbescherming heeft nadere richtlijnen gedefinieerd voor profilering.[115]
Big data kan een belangrijke bijdrage leveren aan de aanvulling van het grote tekort aan betrouwbare informatie in de zorg.[116] Alhoewel de kennis over ziekten en aandoeningen de afgelopen decennia sterk is toegenomen, is de precieze oorzaak, of het samenspel van oorzaken, van de meeste ziekten en aandoeningen niet bekend. Het merendeel kan niet écht genezen worden, hetgeen resulteert in chronische aandoeningen, die vaak alleen symptomatisch kunnen worden behandeld. Van de helft van de behandelingen is het effect onbekend, omdat dit niet onderzocht is. En van de helft die wel onderzocht is, is het resultaat veelal onbetrouwbaar[117].

De WRR onderkent dat er geen overeenstemming bestaat over een eenduidige definitie van*big data* en ziet het meer als een samenspel van ontwikkelingen. Daarbij kan een aantal kenmerken genoemd worden waarbij onderscheid gemaakt kan worden naar de aard van de data, de analysetechnieken en het gebruik[118]:

> **Aard van de data**
> Er is sprake van grote hoeveelheden gegevens die vaak on- of semi-gestructureerd zijn. Daarnaast zijn de gegevens gevarieerd en veelal afkomstig uit verschillende databronnen.

113. Expertgroep Big data en privacy voor minister van Economische Zaken, Licht op de digitale schaduw, verantwoord innoveren met big data. Augustus 2016.
114. Zie paragraaf 6.2.2.
115. WP 29, Geautomatiseerde besluitvorming en profilering (WP 251), advies 2016/679', 03-10-2017.
116. WRR, Ottes, 2016 en Ottes 2017.
117. Ioannidis, J.P.A. 'Why Most Published Research Findings Are False'. Plos Med 2(8):e124.
118. WRR Ottes, 2016, p.19.

Analysetechnieken
De analysetechnieken zijn *data driven*. Dit betekent dat naar patronen gezocht wordt zonder dat vooraf hypothesen zijn opgesteld zoals bij de klassieke aanpak. De resultaten zijn snel beschikbaar en geven daardoor inzicht in het nu: *real-time* c.q. *nowcasting*. Ze kunnen voorspellende waarde hebben: *predictive forecasting*.

Gebruik
De verschillende gegevensbronnen bevinden zich veelal in verschillende domeinen. Dit leidt tot ontschotting van domeinen: gegevens uit het ene domein worden gebruikt voor beslissingen in het andere domein. De resultaten op geaggregeerd niveau kunnen toegepast worden op beslissingen op groeps- of individueel niveau.
In de gezondheidszorg zijn bij al deze kenmerken grote ontwikkelingen gaande. Zo leveren bijvoorbeeld nieuwe *next generation sequencing*-technieken enorme hoeveelheden genetische gegevens die men tracht te relateren aan allerlei andere gegevens, van voeding en gevoeligheid voor luchtvervuiling tot psychische stoornissen. Het gaat daarbij vaak om gegevens die voor een ander doel en binnen een ander domein zijn vastgelegd. Door het op de markt komen van allerlei kleine goedkope sensoren kunnen steeds meer fysiologische parameters, zoals ECG, bloeddruk, geautomatiseerd en continu geregistreerd worden. De gegevens kunnen heel eenvoudig draadloos, bijvoorbeeld via een smartphone, in grote gegevensbestanden vastgelegd worden en gerelateerd worden aan de andere gegevens om hierin naar patronen te zoeken.

2.5.2 Praktijkvoorbeelden

Globaal kunnen vijf categorieën *big data* in de zorg onderscheiden worden[119]:

1. '*Human generated data*': Door zorgverleners in het elektronisch medisch dossier vastgelegde gegevens, aantekeningen, e-mails, ontslagbrieven, enzovoort. Veel van deze gegevens zijn ongestructureerd of semi-gestructureerd.

   Human generated data kunnen ook gebruikt worden voor medisch onderzoek. Een voorbeeld is het initiatief van de Nederlandse neuroloog Bas Bloem, waarbij met en door parkinsonpatiënten, gedurende twee jaar onder meer hart- en hersenactiviteiten worden bijgehouden. Doel is om meer inzicht te krijgen in welke therapie werkt bij de parkinsonpatiënt.[120]

   Big-datatoepassingen zoals deze kunnen leiden tot betere zorg waar parkinsonpatiënten baat bij hebben. Ze kunnen patiënten echter ook kwetsbaar maken. Want als patiënten veel gegevens van zichzelf vrijgeven, vergroot dit hun kwetsbaarheid voor misbruik van die gegevens.

   Om misbruik te voorkomen heeft Bloem samenwerking gezocht met Jacobs, hoogleraar computerbeveiliging en bekend omdat hij regelmatig in de media waarschuwt voor beveiligingsproblemen van databanken. Samen hebben ze een technologie ontwikkeld om de gegevens zo te versleutelen – op basis van polymorfe pseudoniemen – dat ze slechts met toestemming van de patiënt gebruikt kunnen worden. De data zijn bovendien ondergebracht in een aparte stichting met een eigen bestuur. Ondanks de samenwerking met Google-zusterorganisatie Verily is gewaarborgd dat de gegevens niet gedeeld worden met Google.

119. WRR, Ottes. 2016, p. 20.
120. https://www.skipr.nl/blogs/id3215-is-de-patient-klant-of-product%3F.html.

2. Transactiegegevens: declaraties, enzovoort.
3. Biometrische gegevens. Hieronder vallen naast vingerafdrukken en netvliesscans ook bijvoorbeeld röntgenfoto's, CT- en MRI-scans en fysiologische meetgegevens, zoals bloeddruk, hartslag, zuurstofverzadiging van het bloed, enzovoort.
4. *Machine-to-machine*-data: bijvoorbeeld door sensoren gegenereerde gegevens die door bewakingsapparatuur worden verwerkt.
5. Websites en social media: deze omvatten bijvoorbeeld klik- en interactiegegevens ('likes' en dergelijke) van sociale media[121].

De in de vorige paragrafen aangehaalde ontwikkeling van consumenten-eHealth[122] is ook een voorbeeld van een big-dataontwikkeling. Evenals wetenschappelijk onderzoek op grote schaal via zogenoemde frameworks op internet, zoals *ResearchKit* van Apple. In de volgende paragraaf komt dit verder aan bod.

Een mogelijk bijzonder gevoelig voorbeeld in de zorg voor de bescherming van persoonsgegevens en informationele zelfbeschikking is het gebruik van *big data* voor Biobanken. Met gerelateerde gezondheidsgegevens kunnen enorme hoeveelheden gegevens worden gegenereerd met een grote variëteit. *Big data* is daarmee waardevol voor wetenschappelijk onderzoek. De informatie bevat evenwel ook gevoelige gezondheids- en erfelijkheidsgegevens. Personen die lichaamsmateriaal voor onderzoek beschikbaar stellen, moeten erop kunnen vertrouwen dat hun gegevens op een verantwoorde wijze beschermd worden en dat het materiaal gebruikt wordt waarvoor het bedoeld is. Zij geven, na vooraf geïnformeerd te zijn, hun toestemming. Maar waarvoor zij precies toestemming geven, is vooraf niet exact aan te geven. En hoe moet met materiaal van overleden patiënten worden omgegaan? Zij kunnen geen specifieke toestemming meer geven. Een ander belangrijk punt is dat uit het onderzoek van het lichaamsmateriaal informatie naar voren kan komen die voor de betrokken patiënt relevant kan zijn, bijvoorbeeld over het al dan niet hebben van een al dan niet behandelbare erfelijke aandoening. Wil de patiënt hierover geïnformeerd worden?
Een andere – heel bekende – toepassing van *big data* in de zorg is het gebruik voor epidemiologische doeleinden. Het bekendste voorbeeld daarvan is Google Flu c.q. Griep Trends, die de verspreiding van griep *realtime* volgde.[123]
Het model is gebaseerd op griepgerelateerde zoekvragen die gebruikers van Google invoeren. Ook voor Nederland houdt Google dit bij. De klassieke manier voor het bijhouden van de verspreiding van griep is met behulp van peilstations. Zo houden in Nederland sinds 1970 circa veertig huisartsenpraktijken de jaarlijkse griepepidemie bij. In de Verenigde Staten houden de *Centres for Disease Control and Prevention* de gegevens bij. Deze officiële gegevens lopen gemiddeld twee weken achter op de realiteit. Google publiceert de gegevens inmiddels niet meer zoals zij eerder wel deed. Zij verzamelt ze nog wel, maar levert ze nu aan onderzoeksinstellingen, zoals aan de *Columbia University's Mailman School, Boston Children's Hospital* en de *Centres for Disease Control and Prevention.*

121. Zoals Facebook, Twitter, Linkedin, blogs, smartphone apps en dergelijke.
122. RVZ, 2014.
123. www.google.org/flutrends/intl/nl/about/how.html.

In 2009 publiceerden onderzoekers van Google een artikel in Nature, waarin zij aangaven dat de resultaten van Google Flu Trends voor 97% accuraat waren. Echter Butler vond bij een follow-upstudie gepubliceerd in februari 2013 in Nature dat Google er in dat jaar flink naast zat en bijna twee keer zoveel griepgevallen meldde dan de officiële *Centers for Disease Control and Prevention*.[124] Het griepvoorbeeld geeft aan dat men niet blind kan varen op *big data*.
Ook de overheid en zorgverzekeraars gebruiken (steeds vaker) *big data* voor de kwaliteit en doelmatigheid van zorg. Zo gebruikt de Inspectie vGezondheidszorg en Jeugd (IGJ) *big data* voor de selectie van risicovolle zorgaanbieders.
De in deze paragraaf beschreven big-dataontwikkelingen bieden mogelijkheden voor het genereren van gegevens waarmee de grote lacunes in kennis in de zorg opgevuld kunnen worden. Een belangrijke vraag is hierbij hoe dit vorm gaat krijgen. Wie bepaalt? Personen? Private partijen? Overheden? In de volgende paragrafen wordt bezien welke relevante maatschappelijke ontwikkelingen voor informationele zelfbeschikking zich bij private partijen en overheden voordoen.

2.5.3 Eerste bevinding: ook niet-persoonsgegevens relevant

Big data richt zich op slimme analyse van gegevens die bij personen worden verzameld die in zekere mate aan een profiel voldoen. Daarbij kan sprake zijn van persoonsgegevens[125], maar het zullen vaak ook andere gegevens zijn. Ondanks dat in dat geval de wetgeving voor de bescherming van persoonsgegevens niet van toepassing is, kunnen die personen wel gestigmatiseerd worden op grond van hun profiel en daardoor in hun autonomie worden aangetast. Oftewel in de big-datasamenleving kunnen ook niet-persoonsgegevens bedreigend zijn voor de informationele zelfbeschikking, al dan niet in de zorg.
Verder is bij *big data* niet langer het onderscheid relevant tussen bijzondere en niet-bijzondere gegevens.[126]
Met *big data* is het onderscheid tussen persoonsgegevens en niet-persoonsgegeven niet langer doorslaggevend voor de informationele zelfbeschikking. Ook meerdere niet-gezondheidsgegevens kunnen door data te combineren met elkaar wel gezondheidsgegevens opleveren. Het gaat om de kwalificatie van het gebruik van het gegeven. Waarvoor wordt een gegeven gebruikt en hoe ziet dat gebruik eruit?
De vlucht die het fenomeen *big data* neemt, betekent dat beslissers, denkers, beleidsmakers en uitvoerders binnen de gezondheidszorg een debat moeten voeren over de randvoorwaarden waaronder op basis van geautomatiseerde dataanalyse en gevonden correlaties gestuurd kan worden op het handelen van personen.

124. Butler, 2013: 155-6.
125. Zie voor het begrip persoonsgegevens de AVG en bijlage B met de definities.
126. Zie NJV preadvies Moerel & Prins (2016).

2.6 TOENAME PRIVATE AANBIEDERS BUITEN DE ZORG

2.6.1 Inleiding

In paragraaf 2.2.2 zagen we dat uit het door CentERdata uitgevoerde onderzoek blijkt dat van de geënquêteerde Nederlanders 21% zijn persoonlijke gezondheidsomgeving toevertrouwt aan commerciële bedrijven zoals Google en Microsoft. Inmiddels hebben bedrijven als Google, Apple, Samsung en Philips steeds meer grip op persoonlijke gezondheidsgegevens. Begin 2018 werd bekend dat Amazon samen met een vooraanstaande bank en een van de meest kapitaalkrachtige investeringsmaatschappijen ter wereld een bedrijf opzet, dat met nieuwe technologie gezondheidszorg gaat regelen. Om te beginnen voor de eigen werknemers.[127] Kort daarna volgde Apple dit voorbeeld.[128] Deze commerciële ICT-bedrijven zijn inmiddels vaak al machtiger dan veel overheden.
Is er op basis van ontwikkelingen in de praktijk aanleiding om aan te nemen dat er machtige commerciële bedrijven zijn die handel (willen) drijven met gezondheidsgegevens? Zouden daar voorwaarden aan moeten worden gesteld? Zo pleit Jacobs[129] om in lijn met het bestaande verbod op het verhandelen van 'eigen' organen ook het commercieel exploiteren van 'eigen' medische gegevens te verbieden.
Regelmatig komen bedrijven in het nieuws die azen op gezondheidsgegevens. In een artikel over de in Europa afgeblazen lancering van Google Health besprak de New York Times kwesties rondom de bescherming van persoonsgegevens en stelde dat 'patiënten kennelijk Google Health niet wilden gebruiken omdat ze vrezen dat hun persoonlijke gezondheidsinformatie mogelijk niet veilig is als ze in het bezit zijn van een groot technologiebedrijf'.[130] In het Belgische nieuws van 6 oktober 2017 stond dat een groot internationaal farmabedrijf op patiëntendata uit klinieken aast. Het gaat dan om data als hoeveel patiënten met ziekte X worden opgenomen in de ziekenhuizen? Krijgen die patiënten steeds het nieuwste geneesmiddel dat voor de aandoening op de markt is of een ouder, goedkoper middel? Heel wat Belgische ziekenhuizen blijken voor de keuze te staan of ze data over hun patiënten, al dan niet identificeerbaar, verkopen aan een multinational die met farmabedrijven samenwerkt. Het stelt in het licht van het medisch beroepsgeheim de vraag op scherp of data uit ziekenhuizen gebruikt mogen worden met het oog op winst voor private bedrijven.
Het bedrijf in kwestie is QuintilesIMS, wereldwijd een van de grootste dienstverleners in de gezondheidszorg. Het bedrijf monitort onder meer de medicijnenverkoop en begeleidt farmabedrijven bij de commercialisatie van producten. Daarnaast biedt QuitilesIMS diensten aan ziekenhuizen aan. Het bedrijf heeft enkele jaren geleden een Belgische IT-firma overgenomen die individuele analyses maakt voor ziekenhuizen, bijvoorbeeld rond het medicatiegebruik,

127. https://nos.nl/artikel/2215075-de-nieuwe-groeimarkt-voor-techgiganten-gezondheidszorg.html.
128. https://www.icthealth.nl/nieuws/apple-richt-klinieken-medewerkers-op-om-innovaties-testen/.
129. Jacobs, 2015, zie eerder paragraaf 1.6.
130. Lohr, Steve (2008-05-20). "New York Times: Google Offers Personal Health Records on the Web". The New York Times.

inclusief een vergelijking met andere ziekenhuizen. QuintilesIMS stelt alleen gegevens te gebruiken waarmee patiënten niet identificeerbaar zijn.[131]
Handel in gezondheidsgegevens is niet alleen mogelijk via de – door het medisch beroepsgeheim beschermde – medische dossiers van de zorgaanbieders, maar juist ook via persoonlijke gezondheidsomgevingen die beheerd worden door commerciële IT-bedrijven. Kool en Van Est van het Rathenau Instituut waarschuwen in hun essay '*Intieme technologie*' uit het Liberaal Reveil voor de handel in onze hartslag en bloeddruk.[132] Het Rathenau Instituut noemt de opkomst van smartphones, sociale media, sensornetwerken, robotica, virtuele werelden en *big data* 'intieme technologie':[133] technologie nestelt zich in ons, tussen ons, gedraagt zich als ons en weet steeds meer over ons.

In de voorgaande paragrafen kwam de ontwikkeling van opkomende smartphones en de daaraan gerelateerde consumenten-eHealth eveneens aan de orde. Het ligt in de lijn der verwachting dat in de toekomst nog veel meer zaken met kleine, relatief goedkope consumenten-eHealth-apparaatjes gemeten kunnen worden. Hierbij kan gedacht worden aan ECG-monitoring, elektronische stethoscopen, oor- en oogspiegels en longfunctiemeters.[134] Wellicht komt in de nabije toekomst zelfs echoscopie binnen het bereik van de consument. Er bestaat voor de professionele markt reeds een echoscopieapparaat bestaande uit een kleine *ultrasound transducer* verbonden met een smartphone.[135]
Bedrijven verzamelen met behulp van onder andere consumenten-eHealth en het overige internet steeds meer gezondheidsgegevens van personen. Naar gelang een bedrijf over een langere periode gegevens kan verwerken van een persoon, zal de voorspellende waarde van de modellen en gegevens navenant toenemen. Daar staat tegenover dat personen in toenemende mate transparant worden, terwijl de verzameling en verwerking van data zelf weinig transparant zijn. De genoemde zaken maken de consument kwetsbaarder, omdat deze voor controle en begrip van zaken meer is aangewezen op de verantwoordelijke bedrijven en experts.[136]
TNO heeft onderzoek gedaan naar het vertrouwen van personen in bedrijven en diensten[137]. Ten eerste hechten consumenten belang aan de mogelijkheid om te controleren wie wat met hun gegevens doet. Ten tweede hebben personen soms een beperkt vertrouwen in een dienst vooral bij sociale media, maar voelen ze zich min of meer gedwongen om deze diensten te gebruiken door groepsdruk. Ten derde ondernemen personen zelf beschermende acties, maar vinden ze het moeilijk de effectiviteit daarvan in te schatten. Tot slot is een deel van de consumenten onaangenaam getroffen als bedrijven geld verdienen aan gegevens die zij gratis verstrekt hebben.

131. http://www.standaard.be/cnt/dmf20171005_03115572.
132. Kool en Van Est 2014.
133. Van Est, Rerimassie, Van Keulen & Dorren, 2014.
134. Ottes, L. Consumenten-eHealth. A game-changer?! Achtergrondstudie bij het advies Consumenten-eHealth, Raad voor de Volksgezondheid en Zorg, 2015 www.rvz.net.
135. Portable Ultrasound Machine www.mobisante.com.
136. Expertgroep *Big data* en privacy voor minister van Economische Zaken, Licht op de digitale schaduw, verantwoord innoveren met *big data*. Augustus 2016, p. 15.
137. TNO, Privacybeleving op het internet in Nederland, Delft 2015.

2.6.2 Praktijkvoorbeelden

Een probleem bij het gebruik van de hiervoor besproken consumenten-eHealth-apparaatjes en *apps* is dat zij van verschillende leveranciers komen zonder mogelijke integratie van de gegenereerde gegevens. Voor elk apparaatje moet een andere app of website geraadpleegd worden.
Om dit probleem deels op te lossen, hebben bedrijven zoals Apple, Google en Samsung elk hun eigen zogenoemde health-platform ontwikkeld. Een dergelijk platform levert ontwikkelaars van apps gereedschappen, zodat de informatie van verschillende apps geïntegreerd aan de gebruiker getoond kan worden, althans binnen een specifiek platform.
In deze paragraaf komen, naast dergelijke platforms, praktijkvoorbeelden van handel in gezondheidsgegevens aan bod.

Platforms
Het platform van Apple, HealthKit, is in paragraaf 2.3.3 over de persoonlijke gezondheidsomgevingen al even voorbijgekomen. Google heeft zijn eigen platform voor het Android besturingssysteem in de vorm van Google Fit. Verschillende leveranciers maken fitnessgadgets, zoals Android Wear *smartwatches*, die gegevens aanleveren. Bij Samsung heet het platform SAMI. Aangezien Samsung geen eigen besturingssysteem heeft – de smartphones werken met Android – zoekt deze de oplossing in de *cloud*.[138] Gezondheidsgegevens die verschillende apparaatjes produceren, worden opgeslagen in de cloud en daar geanalyseerd en aan de gebruiker getoond.

De verschillende leveranciers lijken verschillende strategieën te hanteren. Zo richt Google zich vooralsnog specifiek op *lifestyle*. In het verleden was er het project Google Health waarin alle gezondheidsgegevens die op verschillende plaatsen door verschillende zorgverleners werden bijgehouden, bijeengebracht werden. Het project sloeg echter niet aan en werd in 2013 gestaakt. Apple werkt samen met bijvoorbeeld de Mayo Clinic in de VS en met ziekenhuisinformatiesysteemleverancier EPIC. Bij HealthSuite van Philips bestaat de 'Suite' uit:

1. een Health Watch;
2. een Body Analysis Scale;
3. Een oorthermometer;
4. een bovenarmbloeddrukmeter;
5. een polsbloeddrukmeter.

Philips hoopt met deze FDA[139] gecertificeerde consumenten-eHealth-toepassingen laagdrempelige producten aan te bieden voor (potentiële) chronisch zieke consumenten en patiënten die dit – mogelijk op aanraden van de zorgverleners die vertrouwen in het FDA-certificaat – gaan aanschaffen.

138. De *cloud* staat voor een netwerk dat met al de computers die erop aangesloten zijn een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan.
139. De Food and Drug Administration, afgekort FDA, is het agentschap van de federale overheid van de Verenigde Staten, dat de kwaliteit van het voedsel en de medicijnen in brede zin controleert.

Verder claimt IBM[140] dat het met zijn IBM Watson AI-platform in staat was om in tien minuten met de juiste diagnose te komen van een zeldzame vorm van leukemie bij een 60-jarige Japanse vrouw, waar menselijke specialisten deze diagnose niet konden stellen. IBM verwacht binnenkort ook een consumentenapp om deze technologie voor het grote publiek beschikbaar te maken.
Er bestaan lacunes in kennis in de zorg, bijvoorbeeld met betrekking tot de effectiviteit van behandelingen. Big-datatoepassingen zoals de *ResearchKit* kunnen mogelijk een bijdrage bieden aan het opvullen hiervan.
Ioannides[141] geeft aan dat naarmate er grotere financiële belangen op het spel staan, de kans op onderzoeksbias toeneemt. Daarnaast sturen financiële belangen ook wat er onderzocht wordt. Zo worden bijvoorbeeld veel grote klinische studies in opdracht van de farmaceutische industrie verricht. Het betreft onderzoek omtrent geoctrooieerde geneesmiddelen. Zodra een geneesmiddel uit patent is, is onderzoek ernaar voor fabrikanten niet meer interessant.
Big-datatoepassingen in de zorg, zoals de *ResearchKit*, moeten op een of andere wijze gefinancierd worden. Wie betaalt, bepaalt. Een belangrijke vraag is dan ook, hoe dit in de praktijk invulling gaat krijgen en wat dit bijvoorbeeld betekent voor de informationele zelfbeschikking van de consument. Indien de financiering grotendeels vanuit de private sector plaatsvindt, zal deze ook invloed hebben op de onderzoeksagenda. De belangen van de private sector hoeven niet parallel te lopen met die van de persoon of in bredere zin met de volksgezondheid, zodat een reële kans bestaat dat de lacunes in kennis selectief en vooringenomen worden opgevuld.

Handel in gezondheidsgegevens
De toenemende versmelting en vernetwerking van mens en technologie betekent dat veel aspecten van ons leven digitaliseren, waardoor er steeds meer intieme gegevens over ons beschikbaar komen via consumenten-eHealth applicaties.

In 2011 kwam de activiteitentracker Fitbit negatief in het nieuws omdat informatie over het seksuele leven van gebruikers via Google te vinden was. De gegevens die het armbandje meet gedurende nacht en dag worden geüpload naar een onlineprofiel van de gebruiker. Uit die gegevens kunnen bepaalde patronen in activiteit worden geïdentificeerd, waaronder ook de seksuele activiteit. Met de standaard privacyinstelling van de profielen bleken alle data van gebruikers zichtbaar, iets waar veel gebruikers zich niet bewust van waren.[142]

Er is een groeiend netwerk van commerciële partijen die deze gegevens verzamelen, verspreiden, verrijken en verhandelen. De meeste personen hebben echter nog nooit van deze bedrijven gehoord. De grootste datahandel vindt voornamelijk achter de schermen plaats; consumenten hebben geen rechtstreeks contact, of contract, met de grote datahandelaren. Voor dergelijke bedrijven biedt transparantie geen concurrentievoordeel; de huidige onzichtbaarheid geeft hun de speelruimte zaken te doen. Gebruikers van commerciële digitale toepas-

140. In de New York Daily van 7 augustus 2016.
141. Ioannidis, J.P.A. Why Most Published Research Findings Are False. plos Med 2(8):e124.
142. https://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/.

singen zijn inmiddels het zicht op de complexe online datahandel grotendeels kwijtgeraakt. Hoewel zij via algemene voorwaarden vaak zelf toestemming geven voor dataverzameling en -verwerking, overzien ze nauwelijks waarvoor ze toestemming geven. Privacyverklaringen[143] worden niet gelezen: praktisch gesproken kosten zij veel te veel tijd. Overigens is het maar de vraag of personen wijzer zouden worden van het daadwerkelijk lezen van de verklaringen, omdat daar in slechts zeer algemene termen wordt beschreven wat er met de gegevens gebeurt. Bijvoorbeeld dat data gedeeld worden met 'partners', voor 'optimalisatie' van de dienstverlening. Hoeveel en welke partners dat zijn en welke informatie externe partijen krijgen, blijft onduidelijk. In de praktijk hebben gebruikers daarom weinig keuze: akkoord gaan. Niet akkoord gaan betekent immers dat ze de dienst niet kunnen gebruiken. Slob en Schilte stellen daarom vast dat instemming deels fictie is geworden, 'want als je niet instemt, kun je maatschappelijk nauwelijks functioneren'.[144]

Personen geven bedrijven niet alleen toestemming om gegevens te verzamelen, maar ook om deze te verwerken en bijvoorbeeld te gebruiken om profielen aan te maken. Door het complexe web van partijen dat hun data verzamelt, deelt en verrijkt, hebben gebruikers geen zicht op de manier waarop de verzamelde en verwerkte informatie bij hen 'terug' komt. Tot welke profielen leiden de analyses van hun gegevens? Welke producten en diensten worden hen op basis daarvan (niet) aangeboden? Doordat de profielen onzichtbaar zijn, weten gebruikers niet hoe ze worden beïnvloed. Het is lastig bezwaar te maken tegen iets dat verborgen blijft.[145]

In 2013 onderzocht het webanalytics-bedrijf Evidon welke gegevens door de twintig populairste gezondheidapps, waaronder Runkeeper en Fitbit, werden gedeeld.[146] Het delen van data met derde partijen bleek de regel te zijn. Met 'derde partijen' worden partijen anders dan de gebruiker en de aanbieder van de website bedoeld. Deze partijen stellen profielen over het surfgedrag samen, die continu worden ververst, aangevuld, gekocht en verkocht op online veilingen.
Een van deze partijen, BlueKai, verkocht bijvoorbeeld 50 miljoen stukjes informatie over individuele voorkeuren van webgebruikers, voor minder dan 10 dollarcent.[147]
Evidon vond meer dan zeventig derde partijen die data verzamelen over de app-gebruikers. Daarbij ging het om gedragsinformatie (zoals de hoeveelheid lichaamsbeweging) en identificerende gegevens (naam, e-mailgegevens, MACadres of IMEI-nummer).
Door deze datahandel zijn bedrijven in staat om steeds gevoeligere informatie af te leiden over consumenten. Naast etniciteit, inkomen, religie en politieke voorkeuren, weten de datahandelaren ook steeds beter hoe het gesteld is met

143. Verhelst 2012.
144. Slob & Schilte, 2014.
145. Hildebrandt & Van Dijk, 2010.
146. A. Kahl, 'A Healthy Data Set', Evidon Blog, 2013. http://www.evidon.com/blog/healthy-data-set.
147. Angwin, 2014.

de gezondheid van gebruikers.[148] Om daarachter te komen wordt informatie uit verschillende bronnen aan elkaar gekoppeld: online, offline en van diverse *wearables.* Dit blijkt bijvoorbeeld uit de informatie beschikbaar over aan BodyMedia verleende patenten. BodyMedia is een startersbedrijf in *health wearables*, dat beschrijft hoe informatiestromen van diverse *wearables* gecombineerd kunnen worden om gebruikers beter te profileren.[149] De slimme armband weet straks bijvoorbeeld wanneer iemand gemiddeld te weinig beweegt, de slimme weegschaal dat iemand te zwaar is en via de voedingsapp wordt duidelijk of iemand te weinig vitaminen en mineralen binnenkrijgt. Uit de combinatie van deze verschillende stukjes informatie valt onder meer af te leiden of de gebruiker kans heeft op het ontwikkelen van diabetes.[150] De patent-informatie spreekt van het opstellen van '*life-o-types*': groepsprofielen die specifiek betrekking hebben op levensstijl.

2.6.3 Eerste bevinding: herstellen van disbalans

Het aantal private aanbieders buiten de zorg neemt toe. Naast – afzonderlijke – persoonlijke gezondheidsomgevingen gaat het om private platformen die het combineren van een aantal verschillende diensten mogelijk maken. Dit impliceert een grotere laagdrempeligheid en maakt het in theorie makkelijker voor iemand met verschillende gezondheidswensen om deze allemaal te adresseren via één platform, buiten de reguliere zorg.

Door big-dataprofilering, ondoorzichtige algoritmen en complexe, onzichtbare online datahandel ontstaat een systematische disbalans tussen de vermogens van bedrijven enerzijds en die van personen anderzijds. Het herstellen van deze disbalans is gewenst. Is de rechtsbescherming van de AVG voldoende? Is aanvullende regulering noodzakelijk? Kool en Van Est[151] menen dat, nu ook onze biologische data op de online datamarkt verhandeld worden, het procedurele gegevensbeschermingsrecht onvoldoende is. De AVG stelt volgens hen slechts de regels en procedures vast onder welke omstandigheden data gedeeld kunnen worden. Daarom bepleiten zij dat het grondrecht op de bescherming van het privéleven aanpassing nodig heeft door niet alleen te beschermen tegen de macht van de Staat, maar ook tegen de datamacht van bedrijven door de online datahandel en de ontstane informatieasymmetrie tussen bedrijven en personen. Grondwetsaanpassingen zijn vaak tijdrovend en moeizaam. In het vervolg van deze dissertatie wordt bezien of er effectievere en minder ingrijpende maatregelen mogelijk zijn om personen te beschermen tegen de datamacht van bedrijven en overheden. Dit gebeurt onder andere door de mogelijkheid te onderzoeken van een verbod op het commercieel verhandelen van gezondheidsgegevens en de inzet van privacy by design.

148. https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be- more.
149. http://www.google.com/patents/US20080319787.
150. http://www.ft.com/cms/s/0/649d96b2-29f0-11e4-8139-00144feabdco.html#axzz3DN7IgX77.
151. Kool en Van Est 2014.

2.7 TOENEMENDE INVLOED OVERHEID OP DE ZORG

2.7.1 Inleiding

In paragraaf 2.2.2 zagen we dat uit het door CentERdata uitgevoerde onderzoek blijkt dat van de geënquêteerde Nederlanders 6,8% zijn persoonlijke gezondheidsomgeving toevertrouwt aan de overheid. Blijkbaar is het vertrouwen in de overheid nog lager dan die in commerciële partijen.
Voor de toenemende invloed van de overheid op de zorg via digitale gegevensstromen gelden nog steeds de inzichten uit het WRR-rapport iOverheid, bijvoorbeeld wat betreft de jeugdzorg in gemeenten.[152] Losse databases en systemen zijn aan elkaar gekoppeld. Informatie stroomt van de ene database naar de andere, van het ene overheidsorgaan naar het volgende. Niemand is verantwoordelijk voor het geheel aan datastromen. Er is geen overzicht, geen overkoepelende visie, weinig transparantie en er zijn weinig mogelijkheden voor burgers om grip te krijgen op hun persoonlijke gegevens. Terwijl bij het verzamelen en koppelen van informatie fouten mét consequenties worden gemaakt.

2.7.2 Praktijkvoorbeelden

De overheid heeft een toenemende invloed op de zorg. Bijvoorbeeld via de decentralisatie van zorg naar het sociale domein in gemeenten, de uitbreiding van bevoegdheden door inlichtingen- en veiligheidsdiensten, politie en justitie, door toezichthouders zoals de IGJ, etc.
Steeds meer gezondheidsgegevens worden in digitale vorm verwerkt en komen steeds vaker buiten de kring van rechtstreeks bij de behandeling betrokkenen terecht. Gemeenten en andere overheden ontvangen gezondheids- en andere persoonsgegevens in het kader van de decentralisaties in de (jeugd)zorg. Het 'DNA' van de gemeenten en andere overheden is niet altijd gelijk aan dat van de zorginstellingen en het opgebouwde 'DNA' van het medisch beroepsgeheim. De regels voor het delen van informatie van een persoon voor overheidsdoeleinden of van patiënten op basis van een medisch dossier waar geheimhouding op rust, is verschillend. Dit blijkt onder andere uit een advies aan de minister van VWS over beveiliging van patiëntgegevens.[153]

Internet is ooit ontstaan als initiatief van de Amerikaanse overheid vanuit strategisch militair oogpunt, dat resulteerde in *arpa* (of *darpa)-net*. Daarna ontwikkelde het zich in de academische wereld. In de vorige paragraaf zagen we dat het web tegenwoordig vooral in handen is van grote ICT-bedrijven. *Big data* maken deze bedrijven machtig. Overheden die toegang hebben tot de door die bedrijven verwerkte persoonsgegevens en die gegevens kunnen combineren met hun eigen gegevens, hebben nog meer macht. De Snowden-affaire liet zien dat de Amerikaanse National Security Agency (NSA) bij internetbedrijven aanwezige persoonsgegevens gebruikt, veelal met medewerking van bedrijven via

152. WRR, iOverheid, 2011.
153. Zie 'Beveiliging van patiëntgegevens', adviesbureau PBLQ, 1 december 2016, Kamerstukken II, 2016-2017, 31 765, nr. 259. https://www.rijksoverheid.nl/documenten/rapporten/2016/12/01/onderzoek-naar-de-beveiliging-van-patientgegevens.

het grootschalig surveillanceprogramma PRISM. Daarmee heeft de NSA rechtstreeks toegang tot de servers van diverse grote aanbieders van internetdiensten zoals Microsoft, Apple, Google, Skype en Facebook. Zo verkrijgt de Amerikaanse dienst volgens Prins niet alleen ontelbare gegevens van klanten van deze bedrijven, maar heeft het ook toegang tot e-mailberichten, gedownloade documenten en chatgesprekken, zonder dat deze klanten daar iets van weten.[154] Via het *Privacy Shield* en adequaatheidsbesluiten van de Europese Commissie probeert de Europese Unie de verwerking met derde, niet-veilige landen, zoals de Verenigde Staten, te reguleren. In de Nederlandse gezondheidszorg worden op grote schaal persoonsgegevens verwerkt door Amerikaanse bedrijven. Er is een groot cultuurverschil tussen Europa en Amerika. In Europa zijn privacy en de bescherming van persoonsgegevens een grondrecht, terwijl die in Amerika veel meer onderhandelbaar zijn.[155]

Overheden zouden encryptie moeten respecteren. Dat stelde Amnesty International 21 maart 2016 ten tijde van de rechtszaak FBI vs. Apple over het verkrijgen van toegang tot de gegevens op een iPhone. Volgens Amnesty moeten mensen door encryptie zichzelf kunnen beschermen tegen datadiefstal en spionage door andere landen, organisaties, bedrijven of andere mensen. Misbruik van positie door de overheid kan tot *Big Brother*-achtige taferelen leiden.

De overheid heeft een dubbele rol. Zij is hoeder én bedreiger van informationele zelfbeschikking, privacy en bescherming van persoonsgegevens. Als hoeder stimuleert zij elektronische inzage door personen in hun aanstaande persoonlijke gezondheidsomgevingen. De overheid probeert ons te behoeden voor frauduleuze praktijken in de zorg, dus is hierin 'hoeder'. Het bedreigende aspect hierin is dat persoonsgegevens worden gebruikt om die fraude op te sporen. Hetzelfde geldt voor het werk van inlichtingendiensten. Daarmee kan de overheid tegelijk ook een bedreiger zijn.

2.7.3 Eerste bevinding: overheid beschermer en bedreiger

De overheid heeft als taak de samenleving te verdedigen tegen cyberdreigingen, maar – gemeentelijke – overheden bezitten zelf tegelijkertijd meerdere databases met gezondheidsgegevens. Bij personen is het vertrouwen in de overheid laag als het gaat om het beheren van gezondheidsgegevens in de vorm van een persoonlijke gezondheidsomgeving. De overheid is steeds vaker zowel beschermer als bedreiger van de zelfbeschikking en bescherming van gezondheidsgegevens. Dit vergt nadere aandacht en onderzoek.

2.8 CONCLUSIE

Wat levert dit hoofdstuk over praktijkontwikkelingen op aan inzichten voor het beantwoorden van de onderzoeksvragen?

154. http://njb.nl/blog/import/de-klank-van-veiligheid.10047.lynkx.
155. Jacobs, 2017.

Informationele zelfbeschikking lijkt in beginsel steeds meer mogelijk voor personen die dit kunnen of willen via persoonlijke gezondheidsomgevingen en patiëntenportalen van zorgaanbieders. Er zijn verschillende typen personen te onderscheiden: 1. degenen die zich zorgen maken over machtsmisbruik; 2. degenen die gegevens niet kunnen of willen 'managen'; 3. degenen die actief zelf persoonsgegevens willen 'managen'. Deze drie te onderscheiden groepen sluiten aan op drie verschillende discoursen van patiëntgerichte zorg volgens Pluut.

De resultaten uit het onderzoek naar praktijkontwikkelingen werpen de vraag op in hoeverre personen echt volledig in vrijheid kunnen kiezen en of zij kunnen weten waarvoor zij kiezen en toestemming geven. Door big-dataprofilering, ondoorzichtige algoritmen en complexe, onzichtbare online datahandel ontstaat een systematische disbalans tussen de machtscapaciteit van bedrijven enerzijds en die van personen anderzijds. Het herstellen van deze disbalans is gewenst.

De in dit hoofdstuk beschreven praktijkontwikkelingen levert naast deze conclusie vragen op over de benodigde wetgeving ter bescherming van gezondheidsgegevens van personen in persoonlijke gezondheidsomgevingen die vaak in handen zijn van (commerciële) organisaties buiten de zorg. De machtscapaciteit van bedrijven en overheden over gezondheidsgegevens vergt tegenmacht, al dan niet op laagdrempelige wijze.
Normering kan ook gestalte krijgen in de applicaties zelf, namelijk via *privacy-by-design*. Deze en andere mogelijkheden kunnen in potentie personen faciliteren bij het beheer van hun gezondheidsgegevens.

In het vervolg van deze dissertatie wordt bezien welke maatregelen mogelijk zijn om personen te beschermen tegen de datamacht van bedrijven en overheden.

3. *Normatief model*

3.1 INLEIDING

In het vorige hoofdstuk besprak ik de over een breed front oprukkende informatietechnologie die het in toenemende mate mogelijk maakt dat personen hun eigen gezondheidsgegevens via een persoonlijke gezondheidsomgeving (laten) beheren. Deze ontwikkelingen vinden overal in de wereld plaats en zijn dus niet te negeren. Deze empirische constatering is evenwel niet het hele verhaal. Dit hoofdstuk gaat in op de vraag naar de aanvaardbaarheid en de risico's op misbruik en oneigenlijk gebruik van de feitelijk ter beschikking komende nieuwe mogelijkheden. Daarmee komt de vraag naar een passend normatief kader aan de orde. Ik sluit me in die zoektocht aan bij een aantal rechtsfilosofen, die praktijkontwikkelingen in het hedendaagse recht analyseren en in goede banen willen leiden.

Het gedachtegoed van deze rechtsfilosofen wordt toegepast op de nieuwe technologische en maatschappelijke ontwikkelingen uit hoofdstuk 2 in het licht van informationele zelfbeschikking.

Over de morele aspecten van zelfbeschikking in onze samenleving is veel geschreven. Bij zelfbeschikking zijn vrijheid en autonomie belangrijke, zij het geen absolute waarden. Niet iedereen is in gelijke mate tot autonomie in staat of bereid. Ook waarden als rechtsbescherming, vertrouwen en de waarde van solidariteit zijn daarbij relevant.
In een democratische rechtsstaat is informationele zelfbeschikking niet alleen een technisch-juridisch begrip. Het gaat om een fundamentele morele waarde. Hierbij maak ik twee kanttekeningen.
In de eerste plaats is het zelfbeschikkingsrecht weliswaar fundamenteel, maar zijn er vaak ook andere morele waarden in het geding. Daarom moet een balans gezocht worden. Kenmerkend voor een gerichtheid op positieve vrijheid is dat negatieve vrijheid wordt gerelativeerd en beperkt. Juist om zelfbeschikking in termen van het vormgeven van het eigen leven te kunnen bevorderen. In het Europese recht speelt in dit verband menselijke waardigheid een rol. Recht op keuzevrijheid kan worden genegeerd indien dit de waardigheid van de persoon aantast of anderszins strijdig is met maatschappelijke normen.[156] Het recht op autonomie dient niet alleen te worden gezien als een negatief afweerrecht, maar

156. Hendriks e.a., 2008, p. 15.

te worden beschouwd in samenhang met andere juridische en ethische waarden, waaronder keuzevrijheid en zelfontplooiing.[157]

In de tweede plaats is informationele zelfbeschikking een veelomvattend en gevarieerd concept. Lang niet altijd zijn specifieke regels en praktijksituaties 'moreel geladen'. Dat neemt niet weg dat systematische erosie van 'de persoonlijke levenssfeer' heel riskant kan zijn.
In dit hoofdstuk laat ik me zowel theoretisch-juridisch als moreel inspireren door Fullers acht regels voor deugdelijke wetten en de sociale theorie van de Amerikaanse rechtssocioloog en -filosoof Selznick. Al veel eerder ontwikkelde Selznick samen met Nonet een verhelderend ontwikkelingsmodel in het recht dat in paragraaf 3.2. verder wordt toegelicht.

Bovendien laat ik mij inspireren door het onderscheid tussen negatieve en positieve vrijheid van Berlin en de contextuele benadering van informationele zelfbeschikking en privacy door Nissenbaum. Op basis van het gedachtegoed van de rechtsfilosofen volgt een normatief model, geordend aan de hand van de volgende vier toetsvragen:

1. menselijke waardigheid;
2. responsieve regulering;
3. contextuele integriteit;
4. rechtsbescherming.

Met een toetsvraag bedoel ik iets anders dan de onderzoeksvragen. Het gaat hierbij om de theoretische, morele en juridische voorwaarden van informationele zelfbeschikking aan de hand waarvan het gedachtegoed van de genoemde rechtsfilosofen door mij worden geordend. Met andere woorden, het om de onderliggende vragen en daarmee de veronderstellingen die mijn normatieve model vormen.

3.2 MENSELIJKE WAARDIGHEID

> *"In het 'Rijk der doelen' heeft alles óf een prijs óf een waardigheid. Wat een prijs heeft, kan worden vervangen; wat daarentegen boven alle geldelijke waarde is verheven, heeft waardigheid. Wat waardigheid heeft, is een doel in zichzelf. Het heeft niet een relatieve, maar een absolute waarde. Het is 'Gegenstand einer unmittelbare Achtung'."* – I. Kant

Uit het rechtsvergelijkende onderzoek naar de bescherming van informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada, dat is uitgevoerd ten behoeve van de Commissie-Franken[158], is gebleken dat het door het Duitse Constitutioneel Hof in 1983 erkende recht op informationele zelfbeschikking werd gebaseerd op het recht op onaantastbaarheid van de menselijke waardigheid en het recht van een ieder op vrije ontplooiing van zijn persoonlijkheid. Ook bij de eerste toetsvraag in dit normatieve kader is de bescherming van de menselijke waardigheid lei-

157. ZonMw Achtergrondstudie, 2014, p. 20.
158. Rapport Staatscommissie Grondwet 2010.

dend. Net zoals dit het geval is bij de lichamelijke zelfbeschikking in de dissertatie van Van Beers.[159] Informationele zelfbeschikking in de zorg is – in belangrijke mate – een machtskritisch concept gericht op vertrouwen in de relatie zorgaanbieder-persoon en het voorkomen van misbruik of oneigenlijk gebruik van persoonsgegevens.
De menselijke waardigheid kan als funderende waarde onder zelfbeschikking worden beschouwd.[160] Menselijke waardigheid is een concept dat in vele filosofische en religieuze tradities is gebruikt. Sinds de Verlichting kan de definitie van menselijke waardigheid van Kant als gezaghebbend worden beschouwd. Alleen de mens voldoet volgens Kant aan deze omschrijving, heeft daardoor absolute waarde en is een doel in zichzelf.

Menselijke waardigheid is overigens een heel plastisch begrip, dat ook kan worden gebruikt om '*en bloc*' tegen een ontwikkeling te zijn. Somsen noemt in zijn Tilburgse oratie (2006) als hoogleraar biotechnologie en recht, het beginsel van de menselijke waardigheid, zodra zij meer omvat dan bescherming van autonomie en vrijheidsrechten, 'repressief', en brengt haar onder meer in verband met 'de conservatief religieuze hoek'. De Kantiaanse lezing van de menselijke waardigheid heeft zelfs een totalitair karakter wanneer het universele gelding wordt toegeschreven, zo stelt Somsen.[161]

Het beginsel van de menselijke waardigheid – ter bescherming van autonomie en vrijheidsrechten – ligt ten grondslag aan de rechten van de mens, vooral zoals dat ontwikkeld is binnen het raamwerk van de Raad van Europa. Van Beers[162] heeft eenuitgebreide internationale rechtsvergelijking gemaakt van het begrip 'menselijke waardigheid'. Het is op grond van dit rechtsbeginsel dat de beschikkingsmacht, die het gevolg is van biomedische technologie, aan banden wordt gelegd. Het is dit beginsel dat volgens Van Beers uiteindelijk de grondslag vormt voor bescherming tegen de risico's van instrumentalisering, commercialisering en uiteindelijk ook dehumanisering van de mens. Deze grondslag is niet alleen voor biomedische technologie, maar ook voor informationele zelfbeschikking relevant. Een analyse van de rechtspraak van het EHRM en een uitvoerige beschouwing van bekende EVRM-jurisprudentie met betrekking tot hulp bij zelfdoding, transseksualiteit, seksuele vrijheid en lijkschennis leidt volgens Van Beers tot de conclusie dat menselijke waardigheid voor het Hof weliswaar uitgangspunt vormt, maar dat de subjectieve invulling ervan door betrokkenen aan invloed blijkt te winnen. Vooral via artikel 8 EVRM: het recht op eerbiediging van het privéleven. Zozeer zelfs dat het Hof een recht op lichamelijke zelfbeschikking inmiddels lijkt te hebben erkend. In hoofdstuk 5 zullen we bezien in hoeverre dit ook voor informationele zelfbeschikking geldt.
Ook de Universele Verklaring van de Rechten van de Mens (UVRM) brengt tot uitdrukking dat de waardigheid van de mens de reden is waarom mensen rechten hebben. De waarde van een mens mag niet worden afgewogen tegen welke praktische overweging dan ook: de mens heeft absolute waarde. In Nederland

159. Van Beers, 2009.
160. Cliteur en Van Wissen, 2012.
161. Somsen, 2006 p. 32 en 37 en Van Beers, p. 673.
162. Van Beers, 2009.

wordt erover gediscussieerd of het concept een meer expliciete rol in de Grondwet zou moeten krijgen.[163]
Vanuit het oogpunt van menselijke waardigheid is zelfbeschikking van groot belang. In het bijzonder zijn zelfbeschikking als keuzevrijheid en zelfbeschikking als zelfontplooiing in deze context essentieel. Menselijke waardigheid heeft echter nog een ruimere en diepere strekking, omdat juist ook degenen die niet volledig zelf kunnen beschikken, zoals kwetsbare, beperkte personen erdoor worden beschermd. Bij de in hoofdstuk 2 beschreven maatschappelijke en technologische ontwikkelingen bleek dat niet iedere persoon, onder iedere omstandigheid, in staat is om informationeel over zichzelf te beschikken. Terwijl onder zelfbeschikking veelal het recht wordt verstaan om het leven naar eigen inzicht in te richten.[164] Het recht op zelfbeschikking kan worden afgeleid uit internationale mensenrechtenverdragen en is inmiddels ook in de jurisprudentie van het EHRM erkend.[165] Op de erkenning van een dergelijk recht, alsmede op de codificering van menselijke waardigheid, is kritiek geuit door Rouvroy en Poullet vanuit de idee dat waarden als menselijke waardigheid, autonomie en zelfbeschikking ten grondslag dienen te liggen aan rechten – voornamelijk het recht op privacy – die deze waarden dienen te verwezenlijken.[166] De waarden zelf dienen evenwel niet gecodificeerd te worden. Desalniettemin kan worden uitgegaan van een recht op zelfbeschikking dat kan worden uitgebreid tot 'informationele zelfbeschikking'. Sinds de intrede van de informatiemaatschappij wordt het begrip zelfbeschikking namelijk niet alleen gebruikt in de context van 'lichaam en leven', maar ook in de context van persoonsgegevens of – iets ruimer geformuleerd – identiteitsgerelateerde informatie.[167] In deze context wordt dat 'informationele zelfbeschikking' genoemd. Dit kan in samenhang worden bezien met het algemeen persoonlijkheidsrecht[168].

Conclusie toetsvraag 1: Menselijke waardigheid – ter bescherming van autonomie en vrijheidsrechten – heeft een ruimere en diepere strekking dan zelfbeschikking, omdat juist ook degenen die niet volledig zelf kunnen beschikken, zoals kwetsbare, beperkte personen, erdoor worden beschermd. Bij de in hoofdstuk 2 beschreven maatschappelijke en technologische ontwikkelingen bleek dat niet iedere persoon onder iedere omstandigheid, in staat is om informationeel over zichzelf te beschikken.

3.3 RESPONSIEVE REGULERING

Fuller pleit voor responsief bestuur.[169] In Nederland is het pleidooi voor een responsief bestuur door Hirsch Ballin uitgewerkt, waarbij hij de eigen verantwoordelijkheid van burgers, het vergroten van de overtuigingskracht van het

163. Mark Düwell's VICI-project onderzoekt of dat gerechtvaardigd is.
164. Hendriks 2006, p. 5.
165. Tysiac t. Polen, nr. 5410/03.
166. Rouvroy en Poullet, p. 52.
167. Van den Hoven en Manders-Huits 2006, nr. 2.
168. Nehmelman 2002.
169. Fuller 1969, p. 23.

overheidsbeleid en het versterken van het handhavingsvermogen sterk benadrukt.[170]
Fuller heeft net als Selznick het ideaal ontwikkeld dat "wetgevers het perspectief moeten innemen van degenen die met de regels moeten werken en leven".[171] Voor mijn theoretisch denkkader is het ideaal van responsieve regulering relevant. Ik combineer het ideaal van responsieve regulering met de overtuiging dat personen in het huidige informatietechnologische tijdperk de garantie dienen te hebben dat informationele zelfbeschikking daadwerkelijk iets voorstelt. In de digitale wereld kan niet volstaan worden met de klassieke juridische bescherming. Als blijkt dat de overheid daartoe een veel actievere rol heeft te vervullen dan in het verleden, dan dient ze zich daarvoor sterk te maken.[172]

Selznick stelt het in stand houden en respecteren van de rechtsstaat voorop. Tegelijkertijd is hij bekend geworden als een voorvechter van responsief recht. Selznick ziet responsief recht als de meest geavanceerde vorm van recht, die openstaat voor veranderingen in de samenleving. Naast de sociale theorie van Selznick heeft Selznick samen met Nonet een theorie ontwikkeld. De theorie van Nonet en Selznick bestaat in de kern uit een typologie van drie ideaaltypen die zijn weergegeven in tabel 1 in de vorm van een ontwikkelingsmodel. Ideaaltypen maken het mogelijk om bepaalde ontwikkelingen en structuren, inclusief de daarachter liggende normen, waarden en motieven, inzichtelijk te maken.[173] Het theoretische model zal worden toegepast zoals het door Nonet en Selznick is bedoeld: als analytisch instrument. De theorie staat ten dienste van de zoektocht naar 'de geest' van het recht[174] De responsieve 'geest' is gericht op de oplossing van problemen en op het realiseren van maatschappelijke effecten. Ook de opvatting dat een juiste toepassing van de regels alléén niet voldoende is, is een centraal uitgangspunt van responsief recht. Nonet en Selznick presenteren – in grote en grove lijnen – een ontwikkelingsmodel van het recht. Repressief recht is inherent instabiel omdat de orde en het gezag niet berusten op instemming maar worden afgedwongen. Gezag bestaat bij de gratie van onderdrukking. Of degenen die aan de regels worden onderworpen daarmee instemmen, is van ondergeschikt belang. Hierdoor ontbreekt het regime van repressief recht aan legitimiteit.
In een systeem van autonoom recht geldt de *'ruleoflaw'*. Er wordt veel belang gehecht aan het volgen van regels en procedures. Het risico doet zich echter voor dat het recht weliswaar keurig volgens de regels wordt toegepast, maar de uitkomst niet als rechtvaardig wordt beschouwd.
In een systeem van responsief recht wordt geen genoegen genomen met rechtmatigheid, maar is rechtvaardigheid de maatstaf waaraan legitimiteit van het recht wordt afgemeten. Daarmee is responsief recht zowel een logisch eindpunt in de ontwikkeling van het recht als een ideaal. Maar ook responsief recht is instabiel omdat het een fluïde scheidslijn kent tussen politiek en recht. Hierdoor

170. Hirsch Ballin 1993, p. 16.
171. Witteveen 2014.
172. Een uitwerking hiervan is de *capability approach* van Nobelprijswinnaar Amartya Sen.
173. Zuurmond, 1994:27.
174. Nonet & Selznick, 2001:17.

loopt responsief recht het risico te vervallen tot repressief recht.[175] In het navolgende zal ik ook ingaan op de vraag waar de grenzen van de inzet op responsief recht liggen. Een risico is immers dat regulering te soepel en mogelijk zelfs te willekeurig wordt. Vandaar dat rechtspraak een belangrijke rol speelt bij het bieden van de noodzakelijke rechtszekerheid.

Drie ideaaltypen van recht volgens Nonet & Selznick, 2001:17 (tabel 1)

	Repressief recht	Autonoom recht	Responsief recht
doel van recht	Orde	Legitimering	Competentie
Legitimiteit	Sociale verdediging en raison d'état	Procedurele eerlijkheid	Substantieve rechtvaardigheid
Regels	Grof en gedetailleerd, maar bindt regelmakers slechts zwak	Uitgebreid: gehouden om zowel regelgevers als de gereguleerden te binden	Onderhevig aan principe en beleid
Redenering	Ad hoc: doelmatig en particularistisch	Strikte navolging van legale bevoegdheid; kwetsbaar voor formalisme en legalisme	Doelgericht; vergroting van cognitieve competentie
Discretie	Vaak voorkomend; opportunistisch	Gebonden door regels; nauwe delegatie	Uitgebreid, maar legt verantwoording af aan doel
Dwang	Uitgebreid; zwak ingeperkt	Beheerst door legale beperkingen	Positieve zoektocht naar alternatieven, e.g. prikkels, duurzame systemen van verplichtingen
Moraliteit	Gemeenschappelijke moraal; legaal moralisme; 'moraal van inperking'	Institutionele moraal; i.e., ingenomen met de integriteit van het legale proces	Burgerlijke moraal, 'moraal van coöperatie'
Politiek	Recht onderhevig aan machtspolitiek	Recht 'onafhankelijk van politiek'; scheiding der machten	juridische en politieke aspiraties geïntegreerd; menging van machten
Verwachtingen van gehoorzaamheid	Onvoorwaardelijk; ongehoorzaamheid an sich gestraft als opstandigheid	Juridisch gelegitimeerde afwijking van regels, e.g. om de validiteit van wetten of bevelen te testen	Ongehoorzaamheid beoordeeld in het licht van substantieve schade; gezien als kwesties van legitimiteit opbrengend
Participatie	Onderdanige nakoming; kritiek als ontrouw	Toegang beperkt door vastgestelde procedures; opkomst van juridische kritiek	Toegang verruimd door integratie van juridische en sociale belangenbehartiging

Conclusie toetsvraag 2: Responsieve regulering staat open voor veranderingen in de samenleving. Fijnmazige regulering past niet bij de snel veranderende, tijd- en plaats onafhankelijke informatietechnologie. In de digitale wereld volstaat klassieke juridische bescherming niet. De overheid heeft daartoe een veel

175. Verberk, 2011.

actievere rol te vervullen dan in het verleden en dient zich daarvoor sterk te maken.

3.4 CONTEXTUELE INTEGRITEIT

Het medisch beroepsgeheim houdt in dat individuele hulpverleners in beginsel geen informatie over hun patiënten aan derden mogen geven. Met andere woorden: medische hulpverleners hebben een zwijgplicht voor de informatie over hun patiënten jegens derden. In de Nederlandse gezondheidswetgeving is het beroepsgeheim onder meer te vinden in de Wet beroepen individuele gezondheidszorg (Wet BIG) en in de Wet geneeskundige behandelingsovereenkomst (WGBO). In de WGBO staat de contractuele relatie tussen patiënt en hulpverlener centraal met verwachtingen ten aanzien van vertrouwelijkheid en beroepsgeheim. Het medisch beroepsgeheim is een leerstuk, bestaande uit normen die te onderscheiden zijn als zwijgplicht en verschoningsrecht. De zwijgplicht geldt tegenover iedereen en is onder andere geregeld in de Wet BIG en de WGBO. Het verschoningsrecht geldt tegenover de rechter, de rechter-commissaris, de officier van justitie en de politie. Het is geregeld in artikel 218 Wetboek van Strafvordering (Sv). Daarbij verwijst het wetsvoorstel tot vaststelling van Boek 1 van het nieuwe Wetboek van Strafvordering naar de uitspraak van de Hoge Raad in 1985[176]. Het wetsvoorstel stelt voor om uitdrukkelijker in de wet op te nemen dat het verschoningsrecht zich niet alleen uitstrekt tot informatie die de betrokkene aan de verschoningsgerechtigde toevertrouwt. Het verschoningsrecht strekt ook uit tot informatie die de verschoningsgerechtigde binnen de vertrouwensrelatie aan de betrokkene geeft. En het verschoningsrecht strekt zich bovendien uit tot eventuele waarnemingen die binnen de vertrouwensrelatie hebben plaatsgevonden. In paragraaf 6.2.3 wordt bij onderdeel 6 over het medisch beroepsgeheim verder ingegaan op deze voorgestelde wetswijziging.

In de gezondheidszorg staat het medisch beroepsgeheim door de vernetwerking van informatie onder druk. Nouwt schreef hier al over in zijn proefschrift van 1997[177]. Inmiddels is onder andere ten gevolge van de in hoofdstuk 2 beschreven maatschappelijke en technologische ontwikkelingen de vernetwerking en de druk op het medisch beroepsgeheim verder toegenomen. Gezondheidsgegevens worden steeds vaker verwerkt buiten de medische context van zorgverlener en patiënt. Het gaat dan ook niet meer zo zeer om patiënten, maar om personen in hun dagelijks leven. Uit het proefschrift van Nouwt blijkt de enorme complexiteit van wettelijke en andere regelingen die van invloed zijn op de omgang met gezondheidsgegevens. Bij verbreding van het domein van patiënten naar personen neemt deze complexiteit alleen maar verder toe. Personen bevinden zich met hun gezondheidsgegevens in vele contexten, waarvan de medische context er slechts één is.

Wat betreft de context van politie en justitie komt er met het wetsvoorstel tot vaststelling van Boek 1 van het nieuwe Wetboek van Strafvordering mogelijk

176. HR 19 november 1985, NJ 1986, 533, met annotatie van 't Hart (Verschoningsrecht).
177. Nouwt 1997.

duidelijkheid ten gunste van een verschoningsrecht, zoals op dit moment vastgelegd in artikel 218 Sv.[178]

Uit het voorgaande blijkt dat ook als de aanpassing van artikel 218 Sv doorgaat, een persoonlijke gezondheidsomgeving ten minste ten dele niet onder het medisch beroepsgeheim valt. Daarom lijkt een 'patiëntgeheim'[179] raadzaam als wettelijke bescherming voor gezondheidsgegevens die buiten het medisch beroepsgeheim vallen. Bijvoorbeeld door naast het toestemmingsrecht van een persoon voor verwerkingsverantwoordelijken van een persoonlijke gezondheidsomgeving tevens een zwijgplicht en een verschoningsrecht bij wet vast te leggen, vergelijkbaar met het medisch beroepsgeheim. Als waarborg[180] voor patiëntgegevens die niet meer door het medisch beroepsgeheim worden beschermd. Met het 'patiëntgeheim' als aanvulling worden de gezondheidsgegevens van personen die er voor hebben gekozen hun gezondheidsgegevens in een persoonlijke gezondheidsomgeving te plaatsen 'automatisch' beschermd. Daardoor kan bijvoorbeeld een opsporingsdienst niet om het verschoningsrecht van de arts en andere geneeskundige hulpverleners heen, alleen doordat de patiënt ervoor gekozen heeft om zijn gegevens beschikbaar te hebben in een persoonlijke gezondheidsomgeving.

De theorie over contextafhankelijkheid van Nissenbaum is een van de invloedrijkste ideeën over privacy en informationele zelfbeschikking van de afgelopen tien jaar.
In deze theorie stelt Nissenbaum dat wij een bepaalde context als zeer bedreigend voor onze privacy kunnen ervaren en een andere helemaal niet. Een voorbeeld: bij een bezoek aan de huisarts verwacht je als patiënt dat de arts je persoonlijke informatie vertrouwelijk behandelt, maar ook dat hij die deelt met specialisten wanneer dat noodzakelijk is. Dat zijn normen die bij deze context horen. Mocht je erachter komen dat jouw arts je gegevens aan een marketingbedrijf heeft verkocht, dan zal je die informatiestroom ongepast vinden en zijn gedrag als een grove privacyschending ervaren: de norm is overtreden, de integriteit van de context huisartsenbezoek geschonden.[181]

Nissenbaum neemt de historisch gegroeide en beproefde contexten als uitgangspunt. De privacynormen zijn in de online wereld hetzelfde als in de offline wereld. Nissenbaum illustreert dit door het zoeken van informatie in een bibliotheek met *googelen* te vergelijken. Ook al verschilt het zoeken op Google met het raadplegen van een bibliotheekcatalogus, er is ook een overeenkomst: beide doe je voor onderzoek, het opdoen van kennis en intellectuele verrijking. Juist deze activiteiten zijn in liberale democratieën belangrijk en moeten niet gehinderd worden door meekijkers of opdringerige autoriteiten.[182]

178. Zie paragraaf 6.2.3 bij medisch beroepsgeheim (onderdeel 6).
179. Dit begrip is voor het eerst gehanteerd in Hooghiemstra & Ippel (2011).
180. Zie over de vraag naar de waarborgfunctie van wetgeving onder andere de Vereniging voor wetgeving en Wetgevingsbeleid, 1995 en Lokin & Zandbergen 2014.
181. Zie M. Martijn en D. Tokmetzis 2016, p. 34.
182. Nissenbaum, 2011.

Nissenbaum ontwikkelt zo dus een 'contextuele' benadering. Deze contextuele benadering sluit mooi aan bij het thema van dit onderzoek 'Informationele zelfbeschikking in de zorg'. De zorgcontext was immers altijd al een relationele context. Een kernvraag is of de kernelementen van deze context gehonoreerd moeten kunnen worden of gehonoreerd blijven als personen hun gezondheidsgegevens laten beheren door partijen met wie zij geen geneeskundige behandelingsovereenkomst hebben. Is dit bijvoorbeeld het geval bij persoonlijke gezondheidsomgevingen? Nissenbaum ziet als uitdaging dat wij om moeten leren gaan met het gegeven dat internet het verzamelen, de analyse en verspreiding van informatie verandert en daardoor de contextuele integriteit van ons sociale leven kan bedreigen. Zij wijst erop dat sommige bedrijven meer macht hebben dan Staten. Wat betreft de overheden zijn de beginselen van goede *governance* en het staatsrecht belangrijk om onderdrukkende krachten in toom te houden, maar zijn die bestand tegen de nieuwe ontwikkelingen?

Hebben personen met persoonlijke gezondheidsomgevingen daarmee echt zelfbeschikking over en inzicht in hun gezondheidsgegevens? Of komt die macht vooral in handen van bedrijven en overheden? Zal er binnen de zorgcontext inderdaad sprake zijn van die gesuggereerde onbegrensde dynamiek? Ziekenhuizen, zorginstellingen en huisartspraktijken blijven waarschijnlijk gegevens beheren. De huidige wet kent een op de zorgverlener rustende dossierplicht[183]. Voor bepaalde typen personen[184] is een 'gedeeld beheer' mogelijk en zinvol. In dat geval duikt de vraag op hoe de bij personen berustende gegevens moeten worden beschermd. Uit de literatuur blijkt dat voor de relatie patiënt-zorgaanbieder het idee van *shared decision-making* een vruchtbaar uitgangspunt is: de patiënt wordt serieus genomen en betrokken bij de behandeling.[185] Voor nieuwe ontwikkelingen binnen de zorgcontext, zoals persoonlijke gezondheidsomgevingen en *big data* zijn aanvullende randvoorwaarden noodzakelijk om de personen te beschermen. Een voorbeeld zou de introductie van een 'patiëntgeheim' kunnen zijn naar analogie van het 'medisch beroepsgeheim'.

Conclusie toetsvraag 3: Vernetwerking van informatie neemt steeds verder toe en zet daarmee ook het medisch beroepsgeheim in toenemende mate onder druk. Het medisch beroepsgeheim kent een individueel en een collectief belang. Wat kan en mag een persoon verwachten dat er gebeurt met zijn gegevens in een persoonlijke gezondheidsomgeving? En wanneer worden de grenzen van de context waarvoor de gegevens bedoeld zijn, overschreden? Is dit bijvoorbeeld het geval bij de machtscapaciteit van bedrijven en overheden in het licht van *big data*?

Op grond van het nieuwe Wetboek van Strafvordering mag op gegevens in een persoonlijke gezondheidsomgeving, afkomstig vanuit het medische dossier onder de verwerkingsverantwoordelijkheid van de zorgaanbieder waarschijnlijk geen beslag gelegd worden door justitie. Justitie kan niet weten welke gegevens in

183. 7:454 eerste lid, BW.
184. Zie de drieslag aan het begin van hoofdstuk 2.
185. Vermunt 2017, Elwin 2014, Stiggelbout 2012, Makoul 2016.

een persoonlijke gezondheidsomgeving afkomstig zijn van medische beroepsbeoefenaren of de persoon. Om die reden zou gesteld kunnen worden dat justitie geen inzage mag krijgen in persoonlijke gezondheidsomgevingen en dat daarmee dit aspect van het eerder besproken patiëntgeheim de facto geregeld lijkt te worden als de voorgenomen wijziging van artikel 218 Sv doorgaat. Zekerheid daarover is er echter ten tijde van het schrijven van deze dissertatie nog niet.

3.5 RECHTSBESCHERMING

Bij rechtsbescherming in het licht van informationele zelfbeschikking gaat het er om dat personen zo veel mogelijk in een positie komen te verkeren waarin zij daadwerkelijk over hun informatie kunnen beschikken. Dat vergt handhaving met transparant en daadkrachtig toezicht en de mogelijkheid tot geschillenbeslechting. Als het even kan geschillenbeslechting op een eenvoudige en toegankelijke wijze.

Naast inspirator voor 'responsieve' regulering zagen we dat Selznick ook inspirator is voor de normatieve vraag of er een toegankelijke en persoonsvriendelijke vorm van rechtsbescherming en klachtbehandeling bestaat. De sociale theorie van Selznick is nog steeds relevant bij een analyse van huidige ontwikkelingen in technologie en samenleving, omdat hij het liberale ideaal van vrijheid verbindt met de noodzaak van een institutioneel ontwerp.
Een institutioneel ontwerp om personen te beschermen en in de praktijk werkelijk zo veel mogelijk echte zelfbeschikking te geven is noodzakelijk. Op dit moment is er nog geen specifiek institutioneel ontwerp voor persoonlijke gezondheidsomgevingen. Algemene wetgeving, zoals de AVG, is van toepassing en verder is het afsprakenstelsel MedMij in ontwikkeling, evenals afsprakenstelsels zoals het Qiy-model.
Een mogelijke aanvulling op de regulering door de overheid is wat in de literatuur wordt aangeduid als gedragsbeïnvloeding door de overheid, oftewel *nudging*. *Nudging* is volgens de WRR:

> *"een slimme, maar niet dwingende wijze van sturen van gedrag, door gebruik te maken van de nieuwe wetenschappelijke kennis over hoe mensen keuzes maken."*[186]

In filosofische zin bouwt Selznick voort op het Amerikaans pragmatisme van Dewey. In deze dissertatie neem ik het in mijn ogen vruchtbare morele perspectief van Selznick als uitgangspunt bij zelfbeschikking in de huidige digitale informatiesamenleving. Naar analogie met de positie die Selznick inneemt in het debat tussen de idealisten en de realisten is hierbij de balans van belang tussen het idealisme van de technologie-optimisten enerzijds en de donkere kant van de informatiesamenleving met cybercrime, datalekken, mogelijk machtsmisbruik en verlies van privacy anderzijds.
Selznick verbindt in zijn '*The Moral Commonwealth*' systematisch de filosofische tradities met sociale theorie en levert daarmee een bijdrage aan de sociale en

186. WRR 2014.

juridische wetenschap van morele ordening. Selznick's sociale theorie is breed, put inzichten uit de sociologie, psychologie en organisatietheorie en probeert een theorie te ontwikkelen van morele personen, instituties en gemeenschappen. Kenmerkend voor zijn morele ordening is een antidogmatische stijl. In het liberalisme-communitarisme-debat beschrijft hij een vorm van liberaal-communitarisme waarbij het liberale ideaal van vrijheid is verbonden met de ethiek van de sociale verantwoordelijkheid.
Zijn kritiek op het pragmatisme van Dewey is dat pragmatisten en liberalen vaak een te optimistisch mens- en maatschappijbeeld hebben. Deze les is moeilijk voor liberalen en pragmatisten.
Net als Hobbes, en in tegenstelling tot Dewey, wijst Selznick op de donkere kant van mensen. Minimaal liberaal legalisme biedt mensen te weinig bescherming, juist waar bescherming dringend noodzakelijk is. Alleen tegenmacht kan macht controleren en die mogelijkheid moet er zijn in iedere morele gemeenschap. Om die reden zijn procedures en structuren belangrijk. Vertaald naar de huidige digitale informatiesamenleving is bescherming en toezicht noodzakelijk om de zelfbeschikking over persoonsgegevens te beschermen. Zowel tegen macht van overheden, als tegen macht van grote gegevensverwerkende bedrijven.
Selznick's responsieve recht staat open voor veranderingen in de samenleving. Fijnmazige regulering past niet bij de snel veranderende, tijd- en plaats onafhankelijke informatietechnologie. Rechtsbescherming en klachtbehandeling is nog niet goed geregeld rond persoonlijke gezondheidsomgevingen in het licht van de geschetste maatschappelijke ontwikkelingen en de geschetste technologische ontwikkelingen. Bij de ontwikkeling van het overwegend private afsprakenstelsel voor persoonlijke gezondheidsomgevingen MedMij en in een eventuele toekomstige wetgeving voor persoonlijke gezondheidsomgevingen dient laagdrempelige rechtsbescherming en klachtbehandeling te worden geregeld.
Een centrale vraag voor overheden is hoe zij als regelgevers dienen te reageren op zowel de uitdagingen als de mogelijkheden van een door technologie gedreven maatschappij, zonder concessies te doen aan legitimiteit, effectiviteit of verzwakking van essentiële voorwaarden voor een stabiele, morele gemeenschap.
Wat betreft de essentiële voorwaarden voor een stabiele, morele gemeenschap is van belang dat misbruik van de geschetste ontwikkelingen wordt tegen gegaan. Zo is bijvoorbeeld denkbaar dat onder de vlag van het ideaal van informationele zelfbeschikking personen wegens bezuinigingsdoeleinden of gemakzucht verplicht worden gesteld hun gegevens te gaan beheren. In de consumentenwereld van vliegen, reizen en verblijven is dit vaak al het geval. Naar analogie kan gesteld worden dat informationele zelfbeschikking een aantrekkelijke gedachte is, maar als ideologie kan leiden tot misbruik of oneigenlijke druk. Welke maatregelen moeten er getroffen worden om dit mogelijk misbruik tegen te gaan?

De inspiratie voor mijn vraag naar rechtsbeschermingsmaatregelen tegen misbruik komt voort uit het werk van Berlin. Hij maakte in zijn essay '*Twee opvattingen van vrijheid*'[187] een belangwekkend onderscheid tussen positieve en negatieve vrijheid. Bij negatieve vrijheid gaat het om een afperking van het eigen domein, waar de Staat en anderen zich niet in mogen mengen: 'vrijheid van'. Vrij zijn

187. Berlin 1959.

van iets te moeten doen dat anderen je opleggen. Anders gezegd: het gaat om een afweerrecht, om zelfbeschikking over de eigen persoonlijke levenssfeer. Hoewel Berlin toegeeft dat dit een beperkte opvatting is, acht hij deze conceptueel helder en daarom bruikbaar in een politieke en morele discussie.
Bij positieve vrijheid gaat het om 'vrijheid tot'. De beschikbaarheid van kansen om de 'auteur van je leven' te zijn en het leven betekenisvol te maken. Positieve vrijheid vraagt juist om stimulering door anderen om zelfbeschikking daadwerkelijk mogelijk te maken. Berlin waarschuwde dat een begrip als positieve vrijheid het gevaar van ideologisch misbruik en van politieke manipulatie op kan roepen. Er is een tendens om 'mogen' al snel in 'moeten' te transformeren, om een recht om te zetten in een plicht, onder de hoede van een zogenaamd 'zorgende' overheid of zorgverzekeraar. Deze waarschuwing is bij persoonlijke gezondheidsomgevingen in de big-datasamenleving nog steeds actueel.

Hoe voorkomen we misbruik bij persoonlijke gezondheidsomgevingen in de big-datasamenleving en hoe kunnen klachten en geschillen van personen laagdrempelig worden beslecht? De overheid reguleert de samenleving steeds minder zelf en steeds minder van bovenaf. Dit vraagstuk wordt verder uitgewerkt in hoofdstuk 7 over rechtsbescherming.
In het huidige systeem is de veronderstelling dat handhaving primair door individuen zelf zal moeten plaatsvinden vanuit het uitgangspunt dat ze zijn geïnformeerd en rechten hebben. Ten onrechte ligt de handhavingsopdracht momenteel primair bij individuen. In navolging van Nissenbaum en het preadvies van Moerel en Prins zou de handhavingsopdracht primair bij verantwoordelijken moeten worden gelegd, bijvoorbeeld door hen te verplichten hun verwerkingen op basis van *privacy-by-design* in te richten.[188]

In aanvulling op laagdrempelige rechtsbescherming en *privacy-by-design* is ook tegenmacht aan datahongerige bedrijven en overheden op hoger niveau noodzakelijk. Door een sterke toezichthouder en de rechterlijke macht, aan de hand van stevige wet- en regelgeving.

Ook vormen van maatschappelijk verantwoord ondernemen bij zorginstellingen en bedrijven, als voorbeeld van geconditioneerde zelfregulering, behoren tot het palet aan mogelijkheden om invulling te geven aan het streven om personen meer zelfbeschikking te geven. Bij persoonlijke gezondheidsomgevingen wordt in het licht van geconditioneerde zelfregulering gewerkt aan het afsprakenstelsel MedMij.[189] Een nieuw institutioneel ontwerp om personen te beschermen en in de praktijk werkelijk zo veel mogelijk echte zelfbeschikking te geven is noodzakelijk. In hoeverre het afsprakenstelsel hieraan kan bijdragen is de vraag, het is een aanzet.

In het voorgaande zijn de praktische randvoorwaarden van het theoretisch model aan de hand van de toetsvragen neergezet. De omgang met de ontwik-

188. Nissenbaum 2011, p. 32–48.
189. Zie www.medmij.nl.

kelingen die ik in hoofdstuk twee hebt geschetst zullen aan deze randvoorwaarden moeten gaan voldoen.

Conclusie toetsvraag 4: Voor informationele zelfbeschikking is zowel transparant en daadkrachtig toezicht als eenvoudige, toegankelijke geschillenbeslechting relevant. Digitale geschillenbeslechting kan daar mogelijk een bijdrage aan leveren. In hoofdstuk 7 wordt verder uitgewerkt welke overige toekomstgerichte aanbevelingen vallen te geven om informationele zelfbeschikking te faciliteren gelet op de opmars van persoonlijke gezondheidsomgevingen.

3.6 CONCLUSIE

In dit hoofdstuk zijn normatieve theorieën toegepast op de nieuwe technologische en maatschappelijke ontwikkelingen in het licht van informationele zelfbeschikking.

De normatieve oorsprong voor informationele zelfbeschikking is volgens het Duitse Constitutioneel Hof de menselijke waardigheid en het recht van een ieder op vrije ontplooiing van zijn persoonlijkheid. In het volgende hoofdstuk over Duitsland wordt dit verder uitgewerkt. Menselijke waardigheid – ter bescherming van autonomie en vrijheidsrechten – heeft een nog ruimere en diepere strekking, dan zelfbeschikking, omdat juist ook degenen die niet volledig zelf kunnen beschikken, zoals kwetsbare, beperkte personen erdoor worden beschermd.

Fuller, Selznick en Nonet hebben laten zien dat responsieve regulering open staat voor veranderingen in de samenleving.

De theorie over contextuele integriteit van Nissenbaum is toegepast op de verbreding van het domein van de zorgverlener-patiënt relatie naar personen in relatie met private partijen en overheden bij persoonlijke gezondheidsomgevingen. Het medisch beroepsgeheim staat steeds verder onder druk. Mogelijk is in aanvulling op het medisch beroepsgeheim een patiëntgeheim noodzakelijk voor persoonlijke gezondheidsomgevingen.

De theorie van Selznick en Nonet leidt in het licht van persoonlijke gezondheidsomgevingen tot de noodzaak van transparant en daadkrachtig toezicht, evenals eenvoudige, toegankelijke geschillenbeslechting. Digitale geschillenbeslechting kan daar mogelijk een bijdrage aan leveren, evenals *privacy by design* en een afsprakenstelsel voor persoonlijke gezondheidsomgevingen.

3.7 VERVOLG

In hoofdstuk 4 is de volgende stap in mijn betoog de juridische uitwerking van het normatieve kader van hoofdstuk 3 voor het begrip informationele zelfbeschikking in Duitsland, inclusief jurisprudentie en dogmatiek.

4. *Informationele zelfbeschikking in Duitsland*

Duitsland is de bakermat van informationele zelfbeschikking. Vandaar dat in dit hoofdstuk het begrip informationele zelfbeschikking met bijbehorende jurisprudentie en dogmatiek wordt uitgewerkt met betrekking tot Duitsland. In hoofdstuk 5 volgt een uitwerking hiervan in Europa. In hoofdstuk 6 volgt de uitwerking voor Nederland in het algemeen en de Nederlandse zorg in het bijzonder.

4.1 HET BEGRIP INFORMATIONELE ZELFBESCHIKKING

Het recht op informationele zelfbeschikking is door het Duitse Constitutioneel Hof omschreven als 'het recht van het individu om in beginsel zelf te beschikken over de openbaarmaking en het gebruik van persoonlijke gegevens'.[190] In hoofdstuk 1 is al opgemerkt dat het Duitse Constitutioneel Hof een genuanceerde benadering koos waarbij het recht op informationele zelfbeschikking niet absoluut kan zijn.
Informationele zelfbeschikking zou volgens Rouvroy en Poullet niet te beperkt moeten worden geïnterpreteerd als alleen de controle op en manipulatie van persoonlijke gegevens.[191] Het 'zelf' is namelijk iets essentieel anders dan 'gegevens' of 'informatie' over het 'zelf'. Informationele zelfbeschikking betekent volgens Rouvroy en Poullet dat een persoon controle heeft over de over hem beschikbare gegevens als een noodzakelijke maar onvoldoende voorwaarde om een bestaan te leven dat zelfbepaald is. Het recht op informationele zelfbeschikking is volgens hen geen vervreemdbaar eigendomsrecht van een persoon over zijn persoonlijke gegevens, zoals dat in de huidige op de markt georiënteerde samenleving wel zou kunnen worden opgevat.

Dommering geeft aan dat het recht op informationele zelfbeschikking in eerste instantie ging over beperking van macht van de overheid en private partijen, maar dat de focus is verschoven naar beginselen van behoorlijke machtsuitoefening.[192] In feite ging daarmee het element van een zelfbeschikkingsrecht verloren. In lijn daarmee is volgens Blok het recht op privacy teruggebracht tot beginselen van behoorlijk gegevensbeheer.[193] Om het aspect van een zelfbeschikkingsrecht weer te hervinden, wil Dommering van het recht op privacy een economisch zelfbeschikkingsrecht maken. Wat overeenstemt in de benaderingen van Dom-

190. Bundesverfassungsgericht (Constitutioneel Hof) 15 december 1983, BVerfGE, 65, 1 (43); 78, 77 (84); 84, 192 (194); 113, 29 (46); 115, 166 (188); 115, 320 (341f.); 117, 202; BVerwG, NJW 2008, 3081; BayVerfGH, DVBI, 2003,861; HambOVG, DÖV 2007,893 (Ls); SächsOVG, NJW 2007,169 (170); BGH, BGHZ 171, 252 (256).
191. Rouvroy en Poullet, in: Gutwirth e.a. 2009, p. 51.
192. Dommering: in Prins 2010, p. 83-99.
193. Blok 2002.

mering, Rouvroy en Poullet is dat privacy en bescherming van persoonsgegevens een uitwerking zijn van informationele zelfbeschikking. Dit proefschrift neemt informationele zelfbeschikking als onderzoeksobject, met privacy en de bescherming van persoonsgegevens als uitwerking hiervan.

4.2 HISTORIE IN DUITSLAND

In het Duitse recht is het recht op informationele zelfbeschikking expliciet omschreven, mede in relatie tot privacy en bescherming van persoonsgegevens, terwijl in het Europese en Nederlandse recht juist de begrippen privacy en de bescherming van persoonsgegevens zijn uitgewerkt, maar 'informationele zelfbeschikking' niet. In de internationale literatuur bestaat verschil van inzicht over de vraag in welke mate het noodzakelijk is deze begrippen met elkaar te verbinden, dan wel van elkaar te onderscheiden.
Met het oog op de onderzoeksvragen wordt in deze paragraaf de Duitse historie van het begrip informationele zelfbeschikking geanalyseerd.

4.2.1 Menselijke waardigheid

De Duitse Federale Grondwet is gebaseerd op de notie van menselijke waardigheid die ook is vastgelegd in artikel 1 GG (Grundgesetz).[194] De menselijke waardigheid is de centrale waarde van de Grondwet en kan niet worden geschonden. Deze notie is terug te voeren op zowel het natuurrecht, als op theorieën betreffende autonomie en zelfbeschikking en de Kantiaanse filosofie.[195]

In de Kantiaanse filosofie staat centraal dat mensen altijd moeten worden behandeld als doel in zichzelf, niet als middel, binnen een morele en sociale omgeving die personen in hun kracht zet en leidt. De Grondwet zelf is ook door deze filosofie gestempeld, wat af te lezen is aan het vastleggen van het persoonlijkheidsrecht. Kenmerkend zijn een vrije ontwikkeling van de menselijke persoonlijkheid, de gerichtheid op waarden, de idee van een democratische en sociale rechtsstaat en de interpretatie van mensenrechten vanuit de menselijke waardigheid.

De algemene waarden vinden hun vertaling in rechtsprincipes. De menselijke waardigheid, in de zin van artikel 1 GG, wordt concreet vertaald in:

– de gelijkwaardigheid van mensen (artikel 3 GG);
– respect voor fysieke identiteit en integriteit (artikel 2, lid 2, GG);

194. Artikel 1 GG:
(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.
(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.
(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.
195. Eberle 1997, p. 967-981.

– respect voor intellectuele en spirituele identiteit en integriteit wat vertaald wordt in de bescherming van de persoonlijkheid (artikel 2 GG);
– limitering van staatsmacht wat met name duidelijk wordt in de garantie van proportionaliteit (artikel 19 GG);
– garantie van een individueel en sociaal bestaan vertaald in het recht op leven (artikel 2, lid 2, GG) en
– de sociale welvaartsstaat (artikel 20, lid 1,(1) GG).

Uit artikel 1 en 2 GG is in de *Landmark* case 'het Census (Volkszählung)-oordeel' het grondrecht op informationele zelfbeschikking afgeleid door het Constitutioneel Hof. Het Constitutioneel Hof heeft in de jurisprudentie uit dezelfde artikelen ook het algemene recht op privacy als grondrecht afgeleid.[196] In artikel 5 GG zijn de, soms met privacy botsende, rechten op vrije meningsuiting, informatievrijheid, censuurverbod, persvrijheid, omroepvrijheid en filmvrijheid vastgelegd. Artikel 10 GG legt het brief-, post- en telefoongeheim vast met inbegrip van bescherming van verzenden van informatie via telecommunicatie.[197] Artikel 13 GG beschermt het huisrecht, met inbegrip van de huiselijke sfeer, wat weer onderdeel van de bescherming van privacy is. In het navolgende is uitgewerkt hoe deze grondrechten zich verhouden tot het persoonlijkheidsrecht en informationele zelfbeschikking.

De Duitse Grondwet plaatst de bescherming van grondrechten centraal. De grondrechten bieden een sfeer waarin personen vrij zijn ten opzichte van de Staat, maar waarbij de overheid ook rechten moet garanderen.[198] Met andere woorden: er zijn grondrechten als 'afweerrechten', waarbij de overheid niet dient in te grijpen in het leven van mensen.[199] De wetgever dient bij het opstellen van wetten rekening te houden met de geest en waarde van grondrechten en dient om die te beschermen ook in private verhoudingen te kunnen ingrijpen.[200] Dit komt tot uitdrukking in de zogenoemde '*Drittwirkung*' (derdenwerking) en horizontale werking van grondrechten.[201] Het Constitutioneel Hof toetst federale wetten aan de Duitse Grondwet. Bij de beperking van grondrechten door de federale wetgever mag de kern van grondrechten niet worden aangetast. Menselijke waardigheid fungeert daarbij als een open concept dat invulling krijgt in de rechtspraktijk.

196. BVerfG 15 januari 1970, BVerfGE 27, 344 (Ehescheidungsakten).
197. BVerfG 20 juni 1984, BVerfGE 67, 157 (172) (G 10); BVerfG 9 oktober 2002, BVerfGE 106, 28 (35) (Mithörvorrichtung); BVerfG 2 maart 2006, BVerfGE 115, 166 (182) (Kommunikationsverbindungsdaten).
198. Schwartz 1989.
199. BVerfG 15 januari 1958, BVerfGE 7, 198 (204) (Lüth); BVerfG 1 maart 1979, BVerfGE 50, 290 (336) (Mitbestimmung); BGHZ 31 oktober 1974, BGHZ 63, 196 (198) (Eingriff an Eigentum an Gemeindestra en); Roßnagel & Schnabel 2008, p. 3535.
200. Zie BVerfG 25 februari 1975, BVerfGE 39, 1 (Schwangerschaftsabbruch I); BVerfG 16 oktober 1977, BVerfGE 46, 160 (Schleyer); BVerfG 8 augustus 1978, BVerfGE 49, 89 (Kalkar I); BVerfG 20 december 1979, BVerfGE 53, 30 (Mülheim-Kärlich); BVerfG 28 mei 1993, BVerfGE 88, 203 (Schwangerschaftsabbruch II); BVerfG 19 oktober 1993, BVerfGE 89, 214 (229) (Bürgschaftsverträge); BVerfG 15 januari 1958, BVerfGE 7, 198 (205 e.v.) (Lüth); BVerfG 23 april 1986, BVerfGE 73, 261 (269) (Sozialplan); Pieroth & Schlink 2008, Rdnr. 181.
201. Pieroth & Schlink 2008.

De menselijke waardigheid uit zich ook in de ontwikkeling van de menselijke persoonlijkheid.[202] In het Censusoordeel verwijst het Hof naar de aard van de mens en de maatschappij. De mens wordt beschouwd als spiritueel-moreel wezen, een geïntegreerd persoon. Daaraan verbonden zijn rationaliteit, zelfbeschikking en morele verplichtingen. De mens is vrij in het handelen, maar dit is wel gebonden aan een zekere moraliteit, waarbij sociale behoeften, persoonlijke verantwoordelijkheid en menselijke solidariteit kernbegrippen zijn. De waardigheid van een persoon staat niet los van de sociale omgeving. Individuele zelfbeschikking is daarom verbonden met concepten als participatie, communicatie en burgerschap. Dit Kantiaanse begrip van menselijke waardigheid heeft daarmee ook een vertaling gekregen in het Duitse persoonlijkheidsrecht. Bij Kant is menselijke waardigheid universaliseerbaar.

Belangrijk is tevens dat het Duitse grondrecht op vrije ontwikkeling van de persoonlijkheid in relatie tot andere persoonlijkheidsrechten moet worden geïnterpreteerd.[203] In tegenstelling tot menselijke waardigheid is 'persoonlijkheid' geen objectieve waarde, en daarom brengt het geen positieve verplichtingen voor de overheid met zich mee. Het algemeen persoonlijkheidsrecht beschermt persoonlijkheidselementen die niet uitdrukkelijk door een bepaald grondrecht worden beschermd, maar essentieel zijn voor de bescherming van de vrije ontwikkeling van de persoonlijkheid.[204] Dit algemeen persoonlijkheidsrecht is op haar beurt niet expliciet in de Grondwet uitgedrukt, maar is als '*nichtenrecht*' (nevenrecht) ontwikkeld in de zin van §823 I BGB.[205] In 1973 wordt het vervolgens door de rechtspraak van het Hof erkend als zelfstandig grondrecht met verwijzing naar het ontbreken van persoonlijkheidsbescherming.[206]

Het algemeen persoonlijkheidsrecht is te onderscheiden in drie componenten:

1. het recht op zelfbeschikking;
2. het recht op zelfbescherming;
3. het recht op zelfexpressie.[207]

Uit het recht op zelfbeschikking zijn door de hoogste Duitse rechter een aantal specifieke rechten afgeleid, zoals:

202. Eberle 1997, p. 967-981.
203. Artikel 2 GG:
(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.
(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.
204. Roßnagel & Schnabel 2008, p. 3534; Zie BVerfG 10 november 1998, BVerfGE 99, 185 (193) (Scientology); BVerfG 25 oktober 2005, BVerfGE 114, 339 (346) (Mehrdeutige Meinungsäusserungen); Hoffmann-Riem 2008, p. 1009-1022.
205. BGHZ 25 mei 1954, BGHZ 13, 334 (Veröffentlichung von Briefen); Kutscha 2012, p. 392.
206. BVerfG 14 februari 1973, BVerfGE 34, 269 (281) (Soraya).
207. Pieroth & Schlink 2006.

– het recht op schuldenvrij beginnen als meerderjarige[208];
– het recht op kennis van de eigen herkomst[209];
– het recht van misdadigers op het respecteren van hun identiteit ten behoeve van resocialisatie[210].

Het recht op zelfbescherming omvat het recht van een persoon om zich terug te trekken, alleen te blijven en de bescherming van medische dossiers[211], bescherming van de ziel en karakter van een persoon[212] en van een vertrouwelijk dagboek[213]. Het recht van zelfexpressie betekent dat een persoon zo veel mogelijk in staat moet worden gesteld over zijn eigen waarneming te beslissen. Dat omvat een bescherming van het recht op eigen beeld[214], het recht op een eigen woord[215] en het omvattende recht op informationele zelfbeschikking[216]. Daarnaast is er in het 'Online-Durchsuchung'-arrest een recht op bescherming van vertrouwelijkheid en integriteit van informatiesystemen geformuleerd, dat onder de noemer van zelfbescherming kan worden gecategoriseerd.[217]

Deze rechten worden betiteld als 'grondrechten', maar zijn dat alleen in de zin van rechten gefundeerd op de Grondwet. Dat is van betekenis voor de beperking van deze rechten.[218] De persoonlijkheidsrechten zijn door het Hof namelijk specifiek ingevuld als antwoord op moderne ontwikkelingen en bijkomende bedreigingen voor de persoonlijkheid.[219] De verhoudingen van deze rechten tot het persoonlijkheidsrecht en tot elkaar zijn niet altijd duidelijk.[220] Het recht op eigen beeld en het recht op eigen woord zijn bijvoorbeeld onderdelen van het recht op informationele zelfbeschikking. Daarnaast vinden informationele zelfbeschikking en de vertrouwelijkheid en integriteit van informatiesystemen ook weer bescherming in andere, benoemde grondrechten. Het persoonlijkheidsrecht is noodzakelijk voor IT-communicatie vanuit op vertrouwen gebaseerde uitoefening van vrijheid.[221] Daarbij gaat het om twee elementen: handelingsvrijheid en een garantie van een persoonlijke sfeer.

Het recht op informationele zelfbeschikking is in Duitsland door het Constitutioneel Hof voor het eerst erkend in het hiervoor al genoemde Volkszählungsurteil

208. BVerfG 13 mei 1986, BVerfGE 72, 155 (170 e.v.).
209. BVerfG 31 januari 1989, BVerfGE 79, 256 (268 e.v.) (Kenntnis der eigenen Abstammung); BVerfG 26 april 1994, BVerfGE 90, 263 (270 e.v.); BVerfG 6 mei 1997, BVerfGE 96, 56 (63) (Vaterschaftsauskunft).
210. BVerfG 5 juni 1973, BVerfGE 35, 202 (235 e.v.) (Lebach); BVerfG 28 juni 1983, BVerfGE 64, 261 (276 e.v.) (Hafturlaub).
211. BVerfG 8 maart 1972, BVerfGE 32, 373 (379) (Ärztliche Schweigepflicht).
212. BVerfG 24 juni 1993, BVerfGE 89, 69 (82 e.v.).
213. BVerfG 14 september 1989, BVerfGE 80, 367 (373 e.v.) (Tagebuch).
214. BVerfG 5 juni 1973, BVerfGE 35, 202 (220) (Lebach); BVerfG 15 december 1999, BVerfGE 101, 361 (380) (Caroline von Monaco II).
215. BVerfG 3 juni 1980, BVerfGE 54, 148 (155) (Eppler).
216. BVerfG 15 december 1983, BVerfGE 65, 1 (Volkszählung).
217. Hoffmann-Riem 2008, p. 1014.
218. Hoffmann-Riem 2008, p. 1014.
219. Eberle 1997, p. 979-981.
220. Hoffmann-Riem 2008, p. 1014.
221. Hoffmann-Riem 2008, p. 1014.

(Censusoordeel) van 1983.[222] Vervolgens heeft dit recht zijn doorwerking gekregen in de Duitse wetgeving, en heeft daarmee ook invloed gehad op de Europese wetgeving.[223] Daarnaast heeft het Hof de inhoud van het recht op informationele zelfbeschikking nog in vele andere zaken nader geïnterpreteerd. Maatschappelijke en technologische ontwikkelingen noodzaken immers telkens weer tot een nieuwe balans in de verhouding tussen de diverse fundamentele rechten en vrijheden. Bij het recht op informationele zelfbeschikking gaat het in andere woorden om responsieve regulering die openstaat voor veranderingen in de samenleving.

Hieronder komt eerst de baanbrekende Census-casus aan de orde. Daarna volgt de daaropvolgende belangrijkste jurisprudentie van het Hof met betrekking tot informationele zelfbeschikking en het persoonlijkheidsrecht. Ten slotte wordt het recht op informationele zelfbeschikking in de Duitse wetgeving verder uitgewerkt.

4.2.2 Censusoordeel van 1983

Voordat het Censusoordeel van 1983 wordt besproken, is het van belang kort het Microcensusoordeel te bespreken.[224] Volgens Eberle is de kern van deze zaken dat indringende en alomvattende vragenlijsten van de bevolking persoonlijkheidsprofielen opleveren die het de Staat mogelijk maken om met behulp van moderne computertechnieken toegang te krijgen tot deze gegevens. De Microcensus-zaak (1969) betreft de grondwettelijkheid van een federale vragenlijst ('microcensus'), opgesteld om een portret van de Duitse bevolking te schetsen.[225] Deze vragenlijst betreft persoonlijke gewoonten, met inbegrip van vakantiepraktijken, werk, levensstandaard en of de moeder werkt of thuisblijft. Het Constitutioneel Hof bepaalt in deze zaak dat naar aanleiding van het voornemen van de overheid om een volkstelling te houden, het niet met de menselijke waardigheid te verenigen is om mensen te dwingen tot volledige registratie van hun persoonlijk leven en dat te catalogiseren, zelfs niet door middel van een anonieme census aangezien een persoon daarmee tot een algemeen toegankelijk object verwordt.[226] Het Hof bepaalt dat de Staat niet mag binnendringen in de binnenste kern van het recht op zelfbeschikking.[227] Een intieme sfeer moet vrij blijven van staatsinperking. Deze 'sfeertheorie' heeft het Hof weer verlaten in het Censusoordeel. Het grondrecht op informationele zelfbeschikking is in deze zaak nog niet geëxpliciteerd, maar wel een aanzet hiertoe. Het Hof constateert in deze zaak evenwel geen ongrondwettelijke inbreuk op het meest intieme terrein, waar de Staat niet mag binnendringen. De vragenlijst betreft weliswaar privézaken maar niet de meest intieme zaken. Daarnaast is voldaan aan de rechtsstatelijke eisen van bepaaldheid en propor-

222. BVerfG 15 december 1983, BVerfGE 65, 1 (Volkszählung).
223. Buitelaar 2012; Abel 2003.
224. Eberle 1997, p. 1001.
225. BVerfG 16 juli 1969, BVerfGE 27, 1 (Mikrozensus).
226. BVerfG 16 juli 1969, BVerfGE 27, 1 (33) (Mikrozensus).
227. BVerfG 16 juli 1969, BVerfGE 27, 1 (35 e.v.) (Mikrozensus).

tionaliteit, waaraan de geplande census van 14 jaar later niet voldoet. De Microcensus is dus door het Hof aanvaardbaar geacht.

Het Hof moet zich veertien jaar later opnieuw uitspreken over een voornemen tot een volkstelling.[228] De door het Duitse Federale Parlement herziene en unaniem aangenomen Wet op de Volkstelling (Volkszählungsgesetzes) bepaalt dat in 1983 een volkstelling onder de Duitse bevolking moet plaatsvinden. Daarbij wordt door middel van meer dan 160 vragen een uitgebreide verzameling persoonlijke gegevens van alle inwoners van Duitsland geregistreerd. Het gaat hierbij om elementaire gegevens als naam, adres, geslacht, huwelijkse staat, aard van het huishouden, religie en werk. Daarnaast wordt gevraagd naar het inkomen, onderwijs, transportmiddel, en wijze van huishouden, inclusief verwarmingsmethode en het gebruik van hulpmiddelen. De verkregen informatie mag worden doorgestuurd naar lokale overheden die de informatie kunnen gebruiken voor bestuurlijke doeleinden, waarbij die informatie bijvoorbeeld kan worden vergeleken met woonregisters. Deze informatie mag lang worden bewaard.[229]

De aangenomen wet leidde tot onverwachte protesten onder de bevolking en burgerinitiatieven. Ook tot rechtszaken ten gevolge van een honderdtal klachten.[230] Hoffmann-Riem geeft aan dat het enkele decennia later wonderlijk is hoeveel ophef deze census heeft gegeven omdat de gevraagde informatie niet indringend lijkt.[231]

Het Constitutioneel Hof is gevraagd een oordeel te geven over de grondwettigheid van de volkstelling. Daarbij bepaalt het Hof dat de census moet worden uitgesteld totdat de grondwettelijkheid daarvan is bepaald. Dit is een uitzonderlijk geval waarbij het Constitutioneel Hof direct oordeelt over een wet. Eberle betoogt dat de Census-zaak een opvallend voorbeeld is van rechterlijk activisme.[232] Ten eerste is de census uitgesteld totdat de grondwettelijkheid is bepaald waarmee het Duitse parlement is gedwongen de wet aan te passen alvorens deze kan worden uitgevoerd. Fundamenteler is dat het Hof een nieuw grondrecht op informationele zelfbeschikking formuleert.
In haar oordeel bepaalt het Hof dat het algemene doel van de census gerechtvaardigd is, maar dat talrijke voorschriften van de Wet op de Volkstelling zonder rechtvaardiging in de fundamentele grondrechten van mensen ingrijpen. De Wet is in strijd met de Duitse Constitutie wegens schending van het recht op informationele zelfbeschikking.[233]

228. BVerfG 15 december 1983, BVerfGE, 65, 1 (Volkszählung).
229. Hornung & Schnabel 2009a, p. 85.
230. BVerfG 15 december 1983, BVerfGE, 65, 1 (43) (Volkszählung); BVerfG 9 maart 1988, BVerfGE 78, 77 (84); BVerfG 11 juni 1991, BVerfGE 84, 192 (194) (Offenbarung der Entmündigung); BVerfG 12 april 2005, BVerfGE 113, 29 (46) (Anwaltsdaten); BVerfG 2 maart 2006, BVerfGE 115, 166 (188) (Kommunikationsverbindungsdaten); BVerfG 4 april 2006, BVerfGE 115, 320 (341 e.v.) (Rasterfahndung II); BVerfG 13 februari 2007, BVerfGE 117, 202 (Vaterschaftsfeststellung); BVerwG NJW 2008, 3081; BayVerfGH, DVBI, 2003, 861; HambOVG, DÖV 2007, 893 (Ls); SächsOVG, NJW 2007, 169 (170); BGH, BGHZ 171, 252 (256); Schwartz 1989, p. 688; zie ook J. Taeger, Die Volkszählung, 1983.
231. Hoffmann-Riem 2008, p. 1009.
232. Eberle 1997, p. 1004.
233. BVerfG 15 december 1983, BVerfGE, 65, 1 (154 e.v.) (Volkszählung); Gola & Schomerus 2012.

Het Hof geeft in zijn overweging aan dat het algemeen persoonlijkheidsrecht het recht van een persoon om in beginsel zelf te beschikken over de openbaarmaking en het gebruik van persoonlijke gegevens garandeert.[234] Op basis hiervan dient men de persoon te beschermen tegen ongelimiteerde verzameling, opslag, gebruik en verzending van persoonsgegevens.

Het Hof besteedt veel aandacht aan zogenoemde persoonlijkheidsprofielen. Hierbij gaat het om het koppelen van gegevensbestanden. Daarmee zijn nieuwe en mogelijk voor personen schadelijke gegevens te genereren. Dat kan een bedreiging vormen voor het recht op informationele zelfbeschikking dat een persoon in staat moet stellen om zelf te beslissen over de te openbaren gegevens.[235] Daarom moeten volgens het Hof waarborgen worden geïntroduceerd, zoals het verbod om bij voorbaat persoonsgegevens op te slaan.

Toch is het recht op informationele zelfbeschikking geen absoluut grondrecht.[236] Het Hof geeft aan dat een persoon geen recht heeft op eigendom van gegevens waardoor er een absolute beheersing van zijn gegevens mogelijk is. Het Hof stelt dat een persoon eerder afhankelijk is van de communicatie met de samenleving waarin hij verkeert. Informatie is, ook al is het gebaseerd op een persoonlijkheid, een reflectie van een sociale realiteit en kan niet uitsluitend worden geassocieerd met een persoon. Een persoon wordt door het Hof in relatie tot de samenleving beschouwd. Het recht op informationele zelfbeschikking is juist van belang met het oog op de sociale en democratische functies van het zelf kunnen beschikken over persoonsgegevens. Tegelijkertijd worden deze functies belemmerd wanneer personen een ongelimiteerd recht hebben om zelf over persoonsgegevens te beschikken, en daardoor zou de vrije wisseling van persoonsgegevens te veel worden gehinderd.[237] Maatschappelijke actoren en het functioneren van de democratie zijn afhankelijk van persoonsgegevens.[238] Daarmee kan er een conflict ontstaan tussen de persoonlijke en sociale componenten van persoonlijke gegevens.[239]
Beperkingen in het recht op informationele zelfbeschikking zijn volgens het Hof alleen toelaatbaar in het geval van een zwaarwegend openbaar belang.[240] Het recht op informationele zelfbeschikking is onderdeel van het algemeen persoonlijkheidsgrondrecht, voorbehouden aan natuurlijke personen ter bevordering van de vrije ontwikkeling van de persoonlijkheid.[241] Het Constitutioneel Hof formuleert een aantal waarborgen ter bescherming van burgers tegen onevenredige inbreuk op het recht op informationele zelfbeschikking. Dit vereist een constitutionele grondslag die aan de rechtsstatelijke eis van normbepaaldheid moet voldoen. De wetgever dient bij deze regelingen ook het rechtsstatelijke beginsel van evenredigheid, ofwel proportionaliteit, in acht te nemen. Als inbreuken nodig worden geacht, moeten burgers in staat zijn

234. BVerfG 15 december 1983, BVerfGE, 65, 1 (154 e.v.) (Volkszählung).
235. Hornung & Schnabel 2009a, p. 87.
236. BVerfG 15 december 1983, BVerfGE, 65, 1 (156 e.v.) (Volkszählung).
237. Eberle 1997, p. 1002-1003.
238. Eberle 1997, p. 1002-1003.
239. Eberle 1997, p. 1002.
240. BVerfG 15 december 1983, BVerfGE, 65, 1 (156 e.v.) (Volkszählung).
241. Hornung & Schnabel 2009a, p. 86.

om te beoordelen of er een risico is voor de persoonlijkheid.[242] Daarom moeten het bereik, de intensiteit en het doel van gegevensverwerking transparant zijn. Vandaar ook dat de grondwettelijke vereisten voor geheime gegevensverzameling nog hoger zijn.

Desondanks betreurt Schwartz de onduidelijkheid die het Hof bij de door rechters en gegevensbeschermingsautoriteiten te maken afweging van belangen laat bestaan.[243] Hij schetst het gevaar dat op dezelfde wijze als bij het persoonlijkheidsrecht elk zwaarwegend openbaar belang kan prevaleren boven dit recht.[244] Dit is het gevolg van een uitspraak van het Hof die de precieze inhoud openlaat aan de praktijk van wetgeving en jurisprudentie[245] en daarmee onvoldoende grondwettelijke bescherming biedt. Anderzijds valt te betogen dat het Hof juist vanuit deze gedachte en de snelle technologische ontwikkelingen een open concept heeft willen creëren in de zin van responsieve regulering.[246]

Het Hof introduceert in haar Censusoordeel ook het concept van 'informationele scheiding van machten'.[247] De Staat moet volgens het Hof niet als één entiteit worden bezien ten aanzien van verzameling en gebruik van persoonlijke gegevens. Vanwege de principes van doelbinding en proportionaliteit, moet het doel van gegevensverzameling worden gespecificeerd op het moment van verzameling en dienen er nooit meer gegevens te worden verzameld dan strikt noodzakelijk voor het te bereiken doel. Het doel wordt gedefinieerd vanuit de specifieke competentie van een bepaalde autoriteit. Dat leidt tot de conclusie dat de Staat niet als één verwerker[248] moet worden gezien. Elke publieke autoriteit moet als afzonderlijke gegevensverwerker worden beschouwd.

Met betrekking tot de Censuswet oordeelt het Hof dat het legitiem is om een census te organiseren voor sociale en economische planning. Die doelen moeten wel duidelijk geformuleerd worden en moeten op evenredige wijze worden bereikt. Bij de grondwettelijke vereisten voor dergelijke beperkingen moet onderscheid worden gemaakt tussen persoonlijke gegevens die in geïndividualiseerde, persoonlijk herkenbare vorm verzameld en verwerkt worden, en anonieme gegevens die bestemd zijn voor statistische doeleinden.[249] Voor de eerste type gegevens moet specifiek worden aangegeven wat er met die gegevens gebeurt. Bij de verzameling van gegevens voor statistische doeleinden kan een precieze en specifieke oormerking van de gegevens niet worden vereist. Daarom moeten er voor dit type gegevens binnen informatiesystemen passende belemmeringen tegenover informatieverzameling en -verwerking staan. Het onderscheid tussen de gegevenstypen was niet meer duidelijk ten gevolge van het doorsturen van de gegevens naar lokale autoriteiten.

242. Hornung & Schnabel 2009, p. 86.
243. Schwartz 1989, p. 692.
244. Verwijzing van Schwartz naar BVerfG 5 juni 1973, BVerfGE 35, 202 (Lebach).
245. Benda 1984, p. 86; Weichert 2008.
246. Gola & Schomerus 2012; Hoffmann-Riem 2008, p. 1022.
247. Hornung & Schnabel 2009a, p. 87.
248. In termen van de AVG 'verwerkingsverantwoordelijke'.
249. BVerfG 15 december 1983, BVerfGE, 65, 1 (159 e.v.) (Volkszählung).

Ook maakt het Hof onderscheid tussen rechtsbeperkende maatregelen die zonder toestemming of tegen de wil van de betrokkenen worden genomen en maatregelen waarbij sprake is van vrijwilligheid.[250] Voor de eerste categorie is in ieder geval een wettelijke machtiging nodig die specifiek, precies en stevig moet zijn. Het Hof laat grote delen van de Censuswet overeind. Het heeft problemen met enkele bepalingen, waaronder een bepaling die het lokale autoriteiten mogelijk maakt om de census-gegevens met lokale woonregisters te vergelijken en daardoor specifiek bepaalde personen te identificeren. Daardoor wordt de kern van de persoonlijkheid geschonden. Daarnaast zijn er onduidelijke bepalingen en bepalingen met een onduidelijk doel voor het verzamelen van informatie die door het Hof terzijde werden geschoven. Uiteindelijk leidt dit tot een nieuwe Censuswet in 1985 en een census in 1987, tot op heden tevens de laatste census in Duitsland.[251]

Kilian en Heussen geven aan dat het Hof in het Censusoordeel de 'sfeertheorie', waarbij onderscheid wordt gemaakt tussen de intieme sfeer, privésfeer en openbare sfeer, heeft verlaten.[252] Volgens Pieroth en Schlink is dat terecht. Dit komt de bescherming van de persoonlijkheid ten goede. Niet langer wordt de indruk gewekt dat de persoonlijkheid als zodanig uit meerdere sferen bestaat.[253] Alle persoonsgegevens verdienen volgens het Hof bescherming. Toch houdt het Hof vast aan een differentiatie met een onaantastbaar bereik van de vormgeving van het privéleven.[254] Daarbij weegt mee hoe zwaar de inbreuk op het recht op informationele zelfbeschikking is. Dit is afhankelijk van de mate van beschikking over de gegevens van de persoon en de kennis over verzameling en verwerking van gegevens. Daarnaast spelen de aard en omvang van de gegevens, aard van verwerking en duur van opslag, voorziene en denkbare gebruiksdoelen en concrete en abstracte gevaren van misbruik een rol. Verder is de tijdfactor van belang voor de zwaarte van de inbreuk. Na verloop van tijd is er grondwettelijk aanspraak mogelijk op verwijdering van gegevens om niet meer met negatieve zaken geconfronteerd te worden.[255] Dit is verder allemaal in het gegevensbeschermingsrecht vastgelegd.

4.2.3 Informationele zelfbeschikking & Constitutioneel Hof

Het Hof leidt het recht op informationele zelfbeschikking af uit de Grondwet, en het algemeen persoonlijkheidsrecht in het bijzonder. De argumentatie die daarachter ligt is als volgt.

> *"Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche*

250. BVerfG 15 december 1983, BVerfGE, 65, 1 (181 e.v.) (Volkszählung).
251. Hornung & Schnabel 2009, p. 85.
252. Weichert 2008.
253. Pieroth & Schlink 1996.
254. BVerfG 15 december 1983, BVerfGE, 65, 1 (142 e.v.) (Volkszählung).
255. BVerfG 5 juni 1973, BVerfGE 35, 202 (Lebach); BVerfG 25 november 1999, NJW 2000, 1859.

Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[256, 257]

Hieruit leidt het Hof het recht op informationele zelfbeschikking af.

"Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[258, 259]

4.2.4 Zes aspecten van het recht op informationele zelfbeschikking

Uit de definitie van informationele zelfbeschikking door het Constitutioneel Hof als 'het recht van een persoon om in beginsel zelf te beschikken over de openbaarmaking en het gebruik van persoonlijke gegevens' zijn zes relevante vragen met betrekking tot informationele zelfbeschikking af te leiden. Vanuit het begrip van informationele zelfbeschikking, verbonden met de waarden van waardigheid en autonomie, zijn namelijk de volgende zes aspecten van het recht op informationele zelfbeschikking te onderscheiden:

1. Gaat het bij informationele zelfbeschikking om het door een persoon kunnen beschikken over al zijn persoonlijke gegevens?
2. Draait het om openbaarmaking van persoonlijke gegevens, waarbij het erom gaat wanneer en binnen welke grenzen informatie zou moeten worden gecommuniceerd naar anderen?
3. Dient deze openbaarmaking op verzoek van een persoon te geschieden?
4. Is het kunnen beschikken over het gebruik van gegevens een kenmerk van informationele zelfbeschikking?

256. BVerfG 15 december 1983, BVerfGE, 65, 1 (154) (Volkszählung).
257. Nederlandse vertaling: 'Het recht op informationele zelfbeschikking is niet verenigbaar met een maatschappelijke ordening en een rechtsstelsel waarin burgers niet meer kunnen weten wie wat wanneer en bij welke gelegenheid over hen weet. Wie onzeker is of afwijkende gedragingen altijd genoteerd en als informatie opgeslagen, gebruikt of doorgegeven worden, zal proberen niet door zulke gedragingen op te vallen. Wie er rekening mee houdt dat deelname aan een massa of een burgerinitiatief direct geregistreerd wordt en dat daardoor risico's kunnen ontstaan, zal mogelijkerwijs besluiten om zijn grondrechten (art. 8, 9 GG) niet te gebruiken. Dit betreft niet alleen het individu, maar ook de gemeenschap, aangezien zelfbeschikking een elementaire functie heeft met betrekking tot het handelen en meewerken van burgers in een democratische gemeenschap.'
258. BVerfG 15 december 1983, BVerfGE, 65, 1 (155) (Volkszählung).
259. 'Daaruit volgt dat de vrije ontwikkeling van de persoonlijkheid onder de moderne omstandigheden van gegevensverwerking vanuit de bescherming van het individu zich verzet tegen onbegrensde verzameling, opslag, gebruik en weergave van zijn persoonlijke gegevens. Deze bescherming wordt vanuit het grondrecht van art. 2(1) jo. Art. 1 (1) GG gegeven. Het grondrecht garandeert daarmee de bevoegdheid van het individu om grondwettelijk zelf over de openbaarmaking en het gebruik van persoonlijke gegevens te beschikken.' Het recht op informationele zelfbeschikking is dus 'het recht van het individu om in beginsel zelf te beschikken over de openbaarmaking en het gebruik van persoonlijke gegevens'.

5. Komt het beginsel van toestemming terug in het concept van informationele zelfbeschikking?
6. Is het recht op privacy en het recht op bescherming van persoonsgegevens als uitwerking, en daardoor als kenmerk, te zien van het recht op informationele zelfbeschikking?

4.2.5 Dogmatiek naar aanleiding van het Censusoordeel

Vanuit de rechtswetenschap is er sinds het Censusoordeel op het concept van informationele zelfbeschikking gereflecteerd.
Zo wordt informationele zelfbeschikking door Rouvroy en Poullet recent als volgt gedefinieerd:

> *"Een individu heeft controle over de over hem beschikbare gegevens als een (noodzakelijke maar onvoldoende) voorwaarde om een bestaan te leven dat zelfbepaald is."*[260]

Hierbij staan niet de gegevens, maar het 'zelf' centraal. Schwartz interpreteert het recht op informationele zelfbeschikking als bescherming van het individu tegen ongelimiteerde verzameling, opslag, toepassing en verzending van persoonlijke gegevens.[261] Daarmee wordt verwerking van persoonlijke gegevens voorkomen die leidt tot het inspecteren en beïnvloeden van personen, waarbij de individuele capaciteit tot zelfbeschikking verloren gaat.

Toch is het volgens Schwartz geen recht op controle over persoonlijke gegevens. Ook Hoffmann-Riem en Albers uiten kritiek op de formulering van een individueel recht op eigen gegevens waarbij het individu zelf kan beslissen over openbaarmaking en gebruik van die gegevens.[262] Gola en Schomerus geven juist aan dat informationele zelfbeschikking inhoudt dat onder de omstandigheden van moderne informatietechnologie eigen beslissingsvrijheid daadwerkelijk mogelijk is.[263]

De fundering van informationele zelfbeschikking in de notie van menselijke waardigheid, zoals naar voren gebracht in het arrest van het Constitutioneel Hof, staat met de marktbenadering in contrast. Commercialisering van persoonsgegevens kan leiden tot een complete commercialisering van de persoonlijkheid.[264] Daarbij is ook van belang dat het Hof informationele zelfbeschikking beargumenteert vanuit het belang van een vrije en democratische samenleving, waarin de autonomie van de persoon ingebed is in de samenleving. Rouvroy en Poullet geven aan dat het Hof dit al in 1954 bepaalde toen ze uitsprak dat een persoon niet op zichzelf moet worden beschouwd, maar altijd in relatie tot anderen.[265] Volgens Schwartz is het aan de Staat om aan deze bescherming

260. Rouvroy & Poullet 2009. p. 51.
261. Schwartz 1989, p. 689-690.
262. Hoffmann-Riem 1998, p. 513, 520; Albers 2005.
263. Gola & Schomerus 2012.
264. Weichert 2001; Voor een uiteenzetting over gevaren van commercialisering voor persoonlijkheidsrechten zie Beuthien & Schmölz 1999, zie Prins 2006.
265. Rouvroy & Poullet 2009. p. 57; BVerfG 20 juli 1954, BVerfG 4, 7 (Investitionshilfe).

invulling te geven door gegevensverwerking zo te organiseren dat persoonlijke autonomie wordt gerespecteerd.[266]

Daarnaast betoogt Vogelsang dat het recht op informationele zelfbeschikking alleen daartoe beschermt dat onder overheidsdwang verzamelde gegevens niet zonder wettelijke basis, dat wil zeggen zonder toestemming van de persoon in kwestie, verzameld en verwerkt mogen worden. Albers vraagt zich af of bij elk overheidsgebruik van persoonsgegevens de grondwettelijke vrijwaring verkregen is.[267] Deze bedenkingen tegen een uit de Grondwet afgeleid informationeel zelfbeschikkingsrecht heeft Vogelsang eveneens geuit.[268]
Wat betreft de fundering van informationele zelfbeschikking schetsen Rouvroy en Poullet een getrapte bescherming van het recht, waarbij de waarden van menselijke waardigheid en autonomie de fundering zijn.[269] Uit deze waarden vloeit het algemeen persoonlijkheidsrecht voort, wat vervolgens weer door het Constitutioneel Hof is geïnterpreteerd als een recht op informationele zelfbeschikking. Het recht op privacy en gegevensbescherming zijn door het Hof geïdentificeerde instrumenten waarmee informationele zelfbeschikking en het algemeen persoonlijkheidsrecht, en uiteindelijk de onderliggende rechten van waardigheid, autonomie en zelfontwikkeling, kunnen worden verwezenlijkt. Dit toont de relevantie van een zoektocht naar de relatie tussen het recht op privacy en gegevensbescherming enerzijds en het recht op informationele zelfbeschikking anderzijds, met een meer specifieke aandacht voor de Duitse, Europese en Nederlandse inkleuring van deze relatie, zoals in deze dissertatie wordt besproken.

Betreffende de fundering van informationele zelfbeschikking betogen Hornung en Schnabel dat het misleidend is om te stellen dat het recht op informationele zelfbeschikking alleen gebaseerd is op het recht op menselijke waardigheid.[270] Informationele zelfbeschikking is een onderdeel van het persoonlijkheidsrecht, overlappend met andere onderdelen.[271] Het persoonlijkheidsrecht is deels gebaseerd op het recht op menselijke waardigheid, waardoor er wel een link is tussen informationele zelfbeschikking en menselijke waardigheid, maar deze is indirect van aard volgens Hornung en Schnabel.

Daarnaast is er nog de relatie tussen informationele zelfbeschikking en bescherming van persoonsgegevens. Hornung en Schnabel zien het Censusoordeel nog altijd als de belangrijkste beslissing inzake gegevensbescherming.[272] Het Hof ziet het recht op informationele zelfbeschikking dan ook uitdrukkelijk als grondrecht op gegevensbescherming.[273] Hoewel er meerdere pogingen zijn ondernomen om dit grondrecht te codificeren op federaal niveau in Duitsland,

266. Schwartz 1989, p. 690.
267. Albers 2005, p. 280.
268. Vogelsang 1987.
269. Rouvroy & Poullet 2009, p. 45-76.
270. Hornung & Schnabel 2009, p. 86.
271. Hornung & Schnabel 2009, p. 86.
272. Hornung & Schnabel 2009, p. 84-85.
273. Weichert 2008.

is een codificering slechts gelukt op het niveau van sommige deelstaten.[274] Wel is er op Europees niveau een grondrecht op gegevensbescherming gekomen.

Met betrekking tot de verhouding tussen informationele zelfbeschikking en privacy, redeneren Hornung en Schnabel dat belangrijke delen van de argumentatie van het Hof gebaseerd zijn op de ideeën van de sociologische systeemtheorie, in het bijzonder van de Duitse socioloog Niklas Luhman. Luhman argumenteert dat fundamentele rechten de functie hebben van beschermer van differentiatie van de maatschappij in subsystemen.[275] De rol van privacy is om de consistentie van de individualiteit van het individu te beschermen, en consistente zelfexpressie is zeer afhankelijk van de scheiding van maatschappelijke subsystemen. Privacy en informationele zelfbeschikking beschermen deze scheidingslijn, door het verspreiden van informatie van de ene sfeer naar de andere sfeer te voorkomen.

Daarmee biedt informationele zelfbeschikking bescherming van contextuele integriteit, zoals bedoeld door Nissenbaum. De bescherming van persoonlijke gegevens wordt essentieel geacht voor een vrije en zelfbepaalde ontwikkeling van een persoon, wat tegelijkertijd een voorwaarde is voor een vrije en democratische orde van communicatie. Daarbij staat het Duitse concept van informationele zelfbeschikking ver af van de idee van privacy als een '*right to be let alone*'.[276] Het is zowel een bescherming tegen inmenging in persoonlijke zaken als een voorwaarde om te participeren in de politieke processen van een democratische rechtsstaat.[277]

Deze paragraaf sluit af met de relatie van informationele zelfbeschikking tot andere grondrechten. Vanuit de interpretatie van informationele zelfbeschikking als 'de persoon is meester over zijn gegevens' kan er een conflict ontstaan met het informatierecht en informatieverwerkingsrecht van derde partijen.[278] Gallwas betoogt dat het recht op toegang tot informatie te veel is beperkt vanwege het doelbindingsbeginsel uit het gegevensbeschermingsrecht, en dat een evenwicht tussen de rechten nodig is vanuit de idee van vrijheid en zelfbeschikking voor de burger.[279] Caspar geeft aan dat de vrijheid van communicatie en pers in balans moeten zijn met informationele zelfbeschikking. De pers is weliswaar vrijgesteld van bepaalde gegevensbeschermingsbepalingen, maar wordt wel beperkt in haar werk, wat uiteindelijk ook zijn weerslag heeft op de grondrechten van burgers en de democratische rechtsstaat. Kutscha brengt in deze discussie in dat vrijheid van communicatie juist gebaat is bij voorwaarden aan deze communicatie.[280] Daarbij volstaat zelfregulering niet, maar dient de Staat dit via wet- en regelgeving af te dwingen.

274. Weichert 2008.
275. Luhmann 1965.
276. Hornung & Schnabel 2009, p. 86. Verwijzing naar Warren & Brandeis 1890.
277. Hornung & Schnabel 2009, p. 86; Simitis 1998; Schwartz 1989, p. 675-701.
278. Gola & Schomerus 2012.
279. Gallwas 1992.
280. Kutscha 2012.

4.3 DUITSE WETGEVING

Het Hof vraagt in het Census-arrest een actieve houding van de wetgevende en uitvoerende machten om organisatorische en procedurele regelingen te implementeren die het risico van een schending van het persoonlijkheidsrecht tegengaan.

> *"Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Dieser mit Verfassungsrang ausgestattete Grundsatz folgt bereits aus dem Wesen der Grundrechte selbst, die als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat von der öffentlichen Gewalt jeweils nur soweit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen unerläßlich ist. Angesichts der bereits dargelegten Gefährdungen durch die Nutzung der automatischen Datenverarbeitung hat der Gesetzgeber mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken."*

De inhoud en grenzen van het recht op informationele zelfbeschikking en het computer-grondrecht zijn niet precies bepaald door het Hof. Het is aan de wetgever om hier, met inachtneming van het proportionaliteitsbeginsel, invulling aan te geven.[281] Er is al een Federale Gegevensbeschermingswet (*Bundesdatenschutzgesetz*) uit 1977 ten tijde van de beslissing voor een volkstelling.[282] Deze wet is volledig gereviseerd na het Census-oordeel. De wetgever heeft deze handschoen opgepakt. Daarnaast zijn er in de jaren negentig vele wetten hervormd, onder andere op het gebied van telecommunicatie.[283] In 1990 is de Gegevensbeschermingswet in werking getreden. In 1995 trad de Gegevensbeschermingsrichtlijn 95/46/EG van de Europese Unie in werking. Duitsland deed er zes jaar over om dit in nationale wetgeving om te zetten. Daarover oordeelde de Europese Commissie dat hiermee geen volledige uitvoering is gegeven aan de richtlijn.[284]

Het recht op informationele zelfbeschikking, dat niet direct te vinden is in de Grondwet, maar wel in de daarop gebaseerde jurisprudentie, is onder andere uitgewerkt in het *Bundesdatenschutzgesetz* en de gegevensbeschermingswetgeving in de verschillende deelstaten.[285] Het gegevensbeschermingsrecht regelt de omgang met persoonsgegevens. Het legt vast onder welke materieelrechtelijke en procesrechtelijke omstandigheden deze gegevens verzameld, verwerkt en gebruikt mogen worden.[286] Het gegevensbeschermingsrecht regelt daarmee het conflict tussen toegankelijkheid en vertrouwelijkheid van persoonsgegevens. De mogelijkheid die het Hof biedt om met het recht op informationele zelfbeschikking tot een autonome beslissing te komen over gegevenstoegang en -gebruik, is via het gegevensbeschermingsrecht ingevuld, door de toestemmingsfunctie of door de mogelijkheid van anonimisering en pseudonimisering.[287]

281. Benda 1984, p. 86.
282. Hornung & Schnabel 2009a, p. 86.
283. Durner 2010. §88 Telekommunikationsgesetz is een uitwerking van het telecommunicatiegeheim (Art. 10 GG). §91 e.v. geven invulling aan het recht op informationele zelfbeschikking.
284. Hornung & Schnabel 2009a, p. 86.
285. Gola & Schomerus 2012.
286. Weichert 2008.
287. Hoffmann-Riem 2008, p. 1013.

Daarnaast zijn er in het straf(proces)recht, burgerlijk (proces)recht en bestuurs(proces)recht vele bepalingen die raken aan het algemeen persoonlijkheidsrecht, informationele zelfbeschikking en privacy.[288] Dit zijn bepalingen die de Grondwettelijke bescherming aan de burger concreet maken, waarbij sprake kan zijn van '*Drittwirkung*' van een grondrecht. Daarbij zijn derden gebonden aan wettelijke bepalingen die de grondrechten van burgers beschermen en aan de grondrechten die van belang zijn bij interpretatie van wettelijke bepalingen.[289] Verder is in de rechtspraak en dogmatiek de horizontale werking van grondrechten ook in het privaatrecht doorgedrongen.[290] De onrechtmatige daad is daarbij van groot belang.[291] Daarnaast kunnen wettelijke bepalingen een basis zijn voor beperking van een grondrecht.

Het grondrecht op bescherming van vertrouwelijkheid en integriteit van informatiesystemen heeft een eerste uitwerking gekregen met de invoering van het nieuwe persoonsbewijs en De-Mail diensten, alsmede de E-Government wet.[292] Deze E-Governmentwet moet zorgen dat elektronische diensten eenvoudiger, gebruiksvriendelijker en efficiënter worden. De authenticiteit van wilsverklaringen moet versterkt worden. Daarnaast heeft de wetgever in de federale wet (*Bundeskriminalamtsgesetz)* de voorwaarden voor online doorzoekingen uit het arrest overgenomen. Volgens Schwartz schiet de wetgeving tegen gebruik van persoonlijke informatie door politie en veiligheidsdiensten echter nog tekort.[293]

4.4 RECHTSPRAAK DUITSLAND

Vergeleken met 1983 zijn de bedreigingen van toezicht op burgers nu veel groter.[294] Waar burgers in Duitsland in de jaren negentig en begin twintigste eeuw de belangstelling voor gegevensbescherming leken te zijn verloren, is die aandacht sindsdien juist verscherpt door de vele beleidsinitiatieven en wetgeving op het terrein van terrorisme- en criminaliteitsbestrijding. Zeker met de mogelijkheden tot controle van en toezicht op niet-verdachte personen is er weer meer publieke aandacht gekomen voor gegevensbescherming. In 2008 resulteert dit onder meer in een nieuwe burgerbeweging, die campagne voert voor privacy en protestmarsen organiseert.[295]

288. Zie o.a. Schwartz 2011; Roßnagel & Schnabel 2008, p. 3534; Durner 2010; §206 StGB bepaalt de straf op schending van het communicatiegeheim; Weichert 2008: Het recht op een eigen beeld is vastgelegd in §§ 22 e.v. KunstUrhG. Het recht op gesproken woord is vastgelegd in §201 StGB.
289. Pieroth & Schlink 2008; Götting 2008; Roßnagel & Schnabel 2008, p. 3534; Zie BVerfG 25 februari 1975, BVerfGE 39, 1 (Schwangerschaftsabbruch I); BVerfG 16 oktober 1977, BVerfGE 46, 160 (Schleyer); BVerfG 8 augustus 1978, BVerfGE 49, 89 (Kalkar I); BVerfG 20 december 1979, BVerfGE 53, 30 (Mülheim-Kärlich); BVerfG 28 mei 1993, BVerfGE 88, 203 (Schwangerschaftsabbruch II); BVerfG 19 oktober 1993, BVerfGE 89, 214 (229) (Bürgschaftsverträge); BVerfG 15 januari 1958, BVerfGE 7, 198 (205 e.v.) (Lüth); BVerfG 23 april 1986, BVerfGE 73, 261 (269) (Sozialplan).
290. Fisahn & Kutscha 2011; BVerfGE 7, 198 (207) (Lüth).
291. Kutscha 2012, p. 393.
292. Schulz 2012.
293. Schwartz 1989, p. 698-701.
294. Hornung & Schnabel 2009a, p. 88.
295. Hornung, Bendrath & Pfitzmann 2010.

Het Constitutioneel Hof heeft een recht op informationele zelfbeschikking geschapen waarmee niet alleen de census is geadresseerd, maar ook om een democratische orde van communicatie is gevraagd die weerstand kan bieden aan de gegevenshonger van vele partijen. De hoekstenen van deze democratische orde van 1983 vormen de basis voor de beslissingen vanaf 2008 inzake het online doorzoeken van computers, automatische nummerplaatherkenning en de gegevensretentie bij telecommunicatie. De onderliggende argumentatie van deze beslissingen is al onderdeel van de redenering in het Censusoordeel. Bij het creëren van een nieuw recht op betrouwbaarheid en integriteit van informatiesystemen is opnieuw verwezen naar de functie van het algemeen persoonlijkheidsrecht om gaten te dichten.

Met het formuleren van het recht op informationele zelfbeschikking geeft het Hof het startsein voor een ontwikkeling van jurisprudentie ten aanzien van het algemeen persoonlijkheidsrecht in combinatie met het recht op privacy, het recht op bescherming van persoonsgegevens en informationele zelfbeschikking. Het recht heeft zich op die manier verder ontwikkeld en gedefinieerd, mede aan de hand van maatschappelijke en technologische ontwikkelingen. Het Hof heeft via arresten op zowel het terrein van het strafrecht, als het privaatrecht en het bestuursrecht, het geformuleerde recht op informationele zelfbeschikking nader uitgewerkt. Hierna volgt een bespreking van de belangrijkste arresten en hun implicaties voor het recht op informationele zelfbeschikking.

4.4.1 Vaderschapstesten

Op privaatrechtelijk terrein is het Hof in 2007 geconfronteerd met een zaak aangaande vaderschapstesten waarin het recht op informationele zelfbeschikking van zowel vader als kind in het geding zijn.[296] Het Hof oordeelt dat de wetgever het voor vaders die twijfelen of ze de biologische vader zijn van hun kind eenvoudiger moet maken om een vaderschapstest uit te laten voeren, op grond van het algemeen persoonlijkheidsrecht van de vader. Moeders moeten dit niet meer zo eenvoudig kunnen weigeren als tot dan toe het geval was. Het algemeen persoonlijkheidsrecht van de moeder is daarbij volgens het Hof niet in het geding. Het recht op informationele zelfbeschikking van het kind natuurlijk wel, want dat wordt door dergelijke wetgeving ingeperkt op het moment dat het kind moet meewerken aan vaderschapstesten. Wel geeft het Hof daarbij aan dat geheime vaderschapstesten nog steeds niet toegestaan zijn, vanwege het recht op informationele zelfbeschikking van het kind.
Deze zaak toont de reikwijdte van het recht op informationele zelfbeschikking. Het gaat in deze zaak niet om een afweerrecht van de twijfelende vaders, maar over hun recht om informatie over hun bloedbanden op te eisen. Het element van zelfbeschikking in het recht van 'informationele zelfbeschikking' dient ruimer te worden opgevat dan alleen het afschermen van de persoonlijke ruimte.

296. BVerfG februari 2007, BVerfGE 117, 202 (Vaterschaftsfeststellung).

4.4.2 Straf(proces)recht

Het grootste deel van de arresten van het Constitutioneel Hof op het terrein van het recht op informationele zelfbeschikking betreft het straf(proces)recht.[297] De lijn van het Hof is daarin consistent. De strafrechtspleging wordt gezien als een zwaarwegend openbaar belang waardoor een inbreuk op het algemeen persoonlijkheidsrecht, en het recht op informationele zelfbeschikking als *lex specialis*[298], gerechtvaardigd kan zijn. Het moet dan wel gaan om een inbreuk die proportioneel is. De wettelijke regeling die de grondslag vormt voor de inbreuk moet voldoen aan de rechtsstatelijke eis van normbepaaldheid. Wanneer aan bovengenoemde eisen is voldaan, acht het Hof toelaatbaar dat burgers die zich weigeren te identificeren tegenover de politie worden bestraft.[299] Ook acht het Hof dan het registreren van gegevens van verdachten op basis van een *Global Positioning System* (GPS) -gegevens van verdachten in een strafzaak geoorloofd, waarbij het Hof wel aangeeft dat de wetgever de vinger aan de pols moet houden als het gaat om de technologische ontwikkelingen.[300] Verder acht het Hof noodzakelijk dat de wetgeving wordt aangepast wanneer de politie nieuwe technische mogelijkheden inzet. Daarbij geeft het Hof als extra beperking dat niet een compleet persoonlijkheidsprofiel mag worden opgesteld aan de hand van GPS-registratie. Aldus is het de politie niet toegestaan alle ritten van personen in haar registratie op te slaan.

Ook het gebruik van vingerafdrukken en het opstellen van een DNA[301]-profiel kan volgens het Hof onder omstandigheden een gerechtvaardigde inbreuk op het recht op informationele zelfbeschikking zijn.[302] Wederom geeft het Hof daarbij aan dat doorslaggevend is of het DNA-profiel wordt gebruikt om een compleet persoonlijkheidsprofiel op te stellen, waarbij ook karaktereigenschappen, ziektes en aangeboren eigenschappen worden opgeslagen. Een dergelijke handeling kwalificeert als een ongeoorloofde inbreuk op het recht op informationele zelfbeschikking. Ook moet het gaan om serieuze feiten. Deze voorwaarde wordt gesteld met het oog op het belang van het gevoel van rechtszekerheid onder burgers. In deze zaak oordeelde het Hof dat de wettelijke regeling inzake genetische vingerafdrukken voldoet aan de grondwettelijke eisen die worden gesteld aan een inbreuk op grondrechten. Het Hof heeft de inbeslagname van e-mails[303] en de registratie van telecommunicatie[304] op vergelijkbare wijze als

297. BVerfG 7 maart 1995, BVerfGE 92, 191 (Personalienangabe); BVerfG 12 april 2005, BVerfGE 112, 304 (Global Positioning System); BVerfG 14 december 2000, BVerfGE 103, 21 (Genetischer Fingerabdruck I); BVerfG 16 juni 2009, BVerfGE 124, 43 (Beschlagnahme von E-Mails); BVerfG 2 maart 2010, BVerfGE 125, 260 (Vorratsdatenspeicherung); BVerfG 4 april 2006, BVerfGE 115, 320 (Rasterfahndung II).
298. *Lex specialis* is Latijn voor bijzondere wetgeving) is een wet, die voorrang krijgt boven de algemene wetgeving.
299. BVerfG 7 maart 1995, BVerfGE 92, 191 (Personalienangabe).
300. BVerfG 12 april 2005, BVerfGE 112, 304 (Global Positioning System).
301. DNA staat voor 'Desoxyribonucleïnezuur', afgekort als DNA (Engels: Deoxyribonucleic acid). Het is een biochemisch macromolecuul dat fungeert als belangrijkste drager van erfelijke informatie in alle bekende organismen.
302. BVerfG 14 december 2000, BVerfGE 103, 21 (Genetischer Fingerabdruck I).
303. BVerfG 16 juni 2009, BVerfGE 124, 43 (Beschlagnahme von E-Mails).
304. BVerfG 2 maart 2010, BVerfGE 125, 260 (Vorratsdatenspeicherung).

in hiervoor beschreven strafrechtelijke zaken, onder omstandigheden toelaatbaar geacht.

Na 11 september 2001

Op het terrein van het strafrecht is het Hof na 11 september 2001 ook geconfronteerd met antiterrorismewetgeving die de privacy steeds verder hebben beperkt. De angst voor terroristische aanslagen heeft de Duitse wetgever ertoe gebracht om een keur aan veiligheidswetten op te stellen die meer bevoegdheden geven aan politie- en veiligheidsdiensten.[305] De meeste wetten hebben een grote impact op vrijheidsrechten van Duitse burgers. De situatie in Duitsland kenmerkt zich door de combinatie van zeer verstrekkende politiebevoegdheden om de binnenlandse veiligheid te garanderen en een groot privacybewustzijn, wat tot uiting komt in krachtige gegevensbeschermings-autoriteiten en privacywetgeving.[306]
In de rechtspraak culmineert deze dubbele houding in belangwekkende arresten, met name van het Constitutioneel Hof. Van februari tot maart 2008 heeft het Constitutioneel Hof een drietal arresten gewezen waarin wettelijke bevoegdheden van politie- en veiligheidsdiensten te ruim werden bevonden. De argumentatie in deze oordelen is gebaseerd op het Censusarrest. De kritiek van het Hof op deze wetgeving: er zijn procedurele gebreken en de formulering is te algemeen om aan de rechtsstatelijke eisen te voldoen.
In een van deze arresten, het '*Rasterfahndungsurteil*' (ofwel het 'Gegevensmining arrest'), oordeelt het Hof naar aanleiding van een klacht van een Marokkaanse oud-student, dat de strafvorderlijke wetgeving in strijd is met het recht op informationele zelfbeschikking.[307] Het gaat hierbij om een zaak in Noordrijn-Westfalen, waarbij de wet het mogelijk maakt om persoonlijke gegevensprofielen van mogelijk islamitische terroristen op te stellen. De '*profiling*' is in deze zaak gebaseerd op gegevens van 5,2 miljoen personen. Volgens het Hof is er disproportionele inbreuk gemaakt op de grondrechten van de klager. Bij het gebruik van 'gegevensprofilering' door de politie moet er sprake zijn van een inbreuk op een wettelijk verankerd belang. Daarbij moet er sprake zijn van een toestand waarin de betreffende situatie met een voldoende mate van waarschijnlijkheid in de nabije toekomst zal resulteren in schade. De algemene situatie in Duitsland na 9/11 vormt volgens het Hof een onvoldoende basis om deze praktijk van 'gegevensproflering' toe te passen. Er dient bewijs voorhanden te zijn van daadwerkelijke voorbereiding van een terroristische aanval. Burgers lopen met de beoogde maatregelen het risico te maken te krijgen met verdere administratieve controlemaatregelen. Bovendien kan het leiden tot stigmatisering van groepen personen in de samenleving, zoals van mensen uit islamitische landen.

In 2008 oordeelt het Hof dat automatische kentekenregistratie, waarbij kentekens worden vergeleken met onderzoeksbestanden, een inbreuk is op het recht op informationele zelfbeschikking.[308] De automatische herkenning van kentekenplaten mag van het Hof niet zonder aanleiding worden uitgevoerd of landelijk worden doorgevoerd. Het beginsel van proportionaliteit in engere zin is niet

305. Hornung & Schnabel 2009b, p. 115.
306. De Hert, De Vries & Gutwirth 2009.
307. BVerfG 4 april 2006, BVerfGE 115, 320 (Rasterfahndung II). Zie Schwartz 2011; Heckmann 2006.
308. BVerfG 11 maart 2008, BVerfGE 120, 378 (Automatisierte Kennzeichenerfassung).

gerespecteerd aangezien de wettelijke machtiging van autoriteiten geautomatiseerde opnames en analyses van kentekenplaten mogelijk maakt, zonder dat er een concrete dreiging is of in het algemeen toegenomen risico's voor rechtsgoederen. Het Hof stelt strenge eisen aan wetgeving inzake automatische registratie van kentekens wegens de grote impact op informationele zelfbeschikking zoals geformuleerd in het Censusoordeel. De wetgeving voldoet in dit geval niet aan de eisen van duidelijkheid en zekerheid, vanwege een gebrek aan vereisten voor het gebruik van de registratie en een ontbrekend duidelijk beschreven doel. Hornung en Schnabel merken op dat het arrest inzake automatische kentekenregistratie de minste controverse geeft van de drie arresten uit 2008. Automatische kentekenregistratie is daarmee niet onmogelijk geworden, maar de wetgeving moet aan strenge eisen voldoen. Naast de twee besproken arresten uit 2008 trekt het 'Online-Durchsuchungen Urteil' de meeste aandacht in de rechtswetenschappelijke literatuur. Dit arrest komt hierna uitvoerig aan de orde.

Samenvattend blijkt dat het belang van het recht op informationele zelfbeschikking in Duitsland is gegroeid sinds het Censusoordeel door de groei van technologische mogelijkheden bij de opsporing en de opkomst van het internationale islamistische terrorisme.

4.4.3 Computer-Grundrecht

In 2008 heeft het Constitutioneel Hof dé '*landmarkcase*' sinds het Censusoordeel gewezen op het terrein van informatie, technologie, persoonlijkheid en menselijke waardigheid: *Online-Durchsuchungen*.[309] Het Hof moest zich uitspreken over een wet van de deelstaat Noordrijn-Westfalen, die het Openbaar Ministerie autoriseerde om met technologische middelen in het geheim toegang te verwerven tot informatiesystemen in het kader van het bestrijden van criminaliteit en terrorisme.[310] Deze wet leidt tot veel debat in politiek en wetenschap.[311] Het Hof bepaalt dat de wet ongrondwettelijk is vanwege het gebrek aan materiële en procedurele waarborgen die vereist zijn ingevolge het Census-arrest.[312] Daarmee volstaat het Hof niet, mede vanwege de bredere discussie over online doorzoekingen in de politiek.[313] Het Hof heeft de nieuwe technologische ontwikkelingen als uitgangspunt genomen in het oordeel en daarbij de enorme impact op de zelfontplooiing van burgers meegewogen.

Volgens het Hof voldoet het bestaande grondwettelijk raamwerk niet om de persoonlijkheid en privacy van burgers te beschermen met het oog op de risico's van het internet.[314] Artikel 10 GG beschermt de geheimhouding van telecommunicatie, maar omvat volgens het Hof niet de online doorzoekingen van

309. BVerfG 27 februari 2008, BVerfGE 120, 274 (Online-Durchsuchungen).
310. Hornung & Schnabel 2009b, p. 116.
311. Hornung & Schnabel 2009b, p. 116.
312. De wet is vervolgens aangepast en alsnog aangenomen. De vraag is echter of deze wet de toetsing van het Hof zal doorstaan. Zie De Hert, De Vries & Gutwirth 2009.
313. Hornung & Schnabel 2009b, p. 116.
314. BVerfG 27 februari 2008, BVerfGE 120, 274 (170 e.v.) (Online-Durchsuchungen); Eifert 2008.

computersystemen, tenzij de autoriteiten VoIP-systemen[315] surveilleren.[316] In de literatuur is gedebatteerd over de vraag of het online doorzoeken van een informatiesysteem in het huis van een persoon het grondrecht op onschendbaarheid van de huiselijke sfeer schendt.[317] Naar het oordeel van het Hof is dit niet het geval, waarbij wordt overwogen dat de feitelijke locatie van informatiesystemen veelal onduidelijk is.[318] Ook is het twijfelachtig of het huisrecht tevens het specifieke probleem van infiltratie van informatiesystemen omvat. De redenering is dat de *hardware* zich dan in een woning moet bevinden, en dat is niet altijd het geval.[319] Het recht op informationele zelfbeschikking voldoet volgens het Hof ook niet om de burger te beschermen tegen het grootschalig gebruik van persoonlijke gegevens via informatiesystemen.[320]

Gegeven deze observaties bepaalt het Hof dat het algemeen persoonlijkheidsrecht ook het grondrecht op een garantie op vertrouwelijkheid en integriteit van informatiesystemen omvat.[321] Het gaat hierbij om bescherming van informatiesystemen die persoonlijke gegevens bewaren in die mate dat het zoeken via een informatiesysteem belangrijke delen van het gedrag of leven van een persoon kan onthullen of zelfs een omvattend beeld van zijn of haar persoonlijkheid. Het gaat hierbij om computers, mobiele telefoons en soortgelijke systemen die een groot bereik aan functies hebben en een variëteit aan persoonlijke gegevens kunnen opslaan en verwerken. Cruciaal is dat het niet beslissend is of het systeem daadwerkelijk persoonlijke gegevens verzamelt of verwerkt, maar of het daartoe in staat is.[322] Het systeem wordt alleen beschermd indien de betrokkene controle op het systeem mag veronderstellen.
Naar het oordeel van Hornung en Schnabel is het door het Hof ontwikkelde grondrecht op vertrouwelijkheid en integriteit van informatiesystemen geen onafhankelijk op zichzelf staand grondrecht, maar een nieuw onderdeel van het algemeen persoonlijkheidsrecht.[323] Dit is ook het geval voor het recht op informationele zelfbeschikking, dat daardoor sterk verbonden is met het genoemde recht, maar tegelijkertijd daarvan is gescheiden vanwege verschillende grenzen aan juridische beperkingen van het recht.

Hornung en Schnabel onderscheiden twee aspecten van het nieuwe grondrecht, namelijk vertrouwelijkheid en integriteit van het systeem. Vertrouwelijkheid heeft betrekking op persoonlijke gegevens, waarmee er een belangrijke overeenkomst bestaat met het recht op informationele zelfbeschikking, ook al zijn de rechtsstatelijke eisen, zoals proportionaliteit en normbepaaldheid, voor inbreuk veel hoger. Het is van toepassing op het moment dat gegevens buiten het systeem om door de autoriteiten worden verzameld. Bij de integriteit van het systeem,

315. VoIp betekent 'Voice-over-Internet-Protocol. Praktisch: bellen over een computernetwerk, zoals internet.
316. BVerfG 27 februari 2008, BVerfGE 120, 274 (182 e.v.) (Online-Durchsuchungen).
317. Zie bijvoorbeeld Hornung 2007.
318. BVerfG 27 februari 2008, BVerfGE 120, 274 (191 e.v.) (Online-Durchsuchungen).
319. Hoffmann-Riem 2008, p. 1021.
320. BVerfG 27 februari 2008, BVerfGE 120, 274 (196 e.v.) (Online-Durchsuchungen).
321. BVerfG 27 februari 2008, BVerfGE 120, 274 (166 e.v.) (Online-Durchsuchungen).
322. Hornung & Schnabel 2009b, p. 116.
323. Hornung & Schnabel 2009b, p. 116.

gaat het om bescherming tegen ongeautoriseerd gebruik van het systeem wat betreft capaciteit, functie en geheugeninhoud. Hierbij is het niet relevant of daarbij persoonlijke gegevens zijn betrokken. Volgens Hornung en Schnabel resulteert deze bescherming in een verbeterde positie van burgers.[324]

De geheime infiltratie van een informatiesysteem door de overheid, waarmee het gebruik van het systeem gemonitord kan worden en opslagmedia kunnen worden gelezen, is grondwettelijk alleen toegestaan als er feitelijk bewijsmateriaal is voor een specifieke bedreiging.[325] Daadwerkelijk belangrijk zijn volgens het Hof bijvoorbeeld het menselijk lichaam en leven, en de persoonlijke vrijheid. Ook kan infiltratie gerechtvaardigd zijn wanneer de basisprincipes van de Staat, of van het menselijk bestaan worden bedreigd. Infiltratie kan reeds worden gerechtvaardigd als zich nog niet met voldoende waarschijnlijkheid laat vaststellen of het gevaar in de nabije toekomst intreedt. Er hoeft geen concreet gevaar bewezen te worden, maar alleen feiten die een indicatie geven van het gevaar. Dat gevaar moet dan wel in de nabije toekomst kunnen optreden en er moet een connectie zijn met de onderzochte individuen. De wet die machtigt tot een dergelijke ingreep, moet bepalingen bevatten om de kern van het privéleven te beschermen.[326]
Op het moment dat de Staat zich kennis verschaft van de inhoud van internetcommunicatie op de daarvoor technisch aangewezen manier, is dat uitsluitend een inbreuk op artikel 10, lid 1, GG wanneer de overheidsinstantie niet door communicatiedeelnemers tot kennisname is geautoriseerd.[327] Neemt de overheid op internet openbaar toegankelijke communicatie waar, of neemt ze deel aan openbaar toegankelijke communicatie, dan maakt ze in principe geen inbreuk op grondrechten.

Het Hof geeft met *Online-Durchsuchungen* vervolg aan het Census-arrest, en past dezelfde uitgangspunten toe op het verzamelen van informatie met behulp van verder ontwikkelde informatietechnologie. Het Hof heeft het concept van onaantastbare bescherming van het kerndomein van het privéleven verder willen brengen, maar volgens veel rechtswetenschappers had hij dat beter kunnen doen onder de noemer van het recht op informationele zelfbeschikking.[328] Naar de mening van Lepsius is het arrest risicovol voor het recht op informationele zelfbeschikking, omdat het beschermingsbereik van dit grondrecht wordt verengd om zo ruimte te scheppen voor een nieuw grondrecht.[329] Alsof het Hof het niet meer aan het recht op informationele zelfbeschikking toevertrouwde om de nieuwe technologische mogelijkheden het

324. Hornung & Schnabel 2009b, p. 116.
325. BVerfG 27 februari 2008, BVerfGE 120, 274 (246 e.v.) (Online-Durchsuchungen).
326. Het Hof heeft dit uitgewerkt in een oordeel over surveillance van privéhuizen, waarbij surveillance moest worden onderbroken vanwege uitingen van diepste gevoelens of seksualiteit: BverfG, 3 maart 2004, BVerfGE 109, 279 (311 e.v.) (Gro er Lauschangriff). Met verzameling van gegevens via systemen is dat alleen mogelijk achteraf, en moet bepaalde gegevens achteraf verwijderd worden die betrekking heeft op het kernbereik van het privéleven. Het is alleen nog niet duidelijk wie dit moet doen en binnen welke tijd. Hornung & Schnabel 2009, p. 117.
327. BVerfG 27 februari 2008, BVerfGE 120, 274 (182 e.v., 290 e.v., 308 e.v.) (Online-Durchsuchungen).
328. Zie Kutscha 2012, p. 391.
329. Lepsius 2008, p. 31.

hoofd te bieden. Volgens Britz is het schadelijk dat het Hof het recht op informationele zelfbeschikking heeft gereduceerd tot het onbeduidende kleine zusje van het nieuwe grondrecht. Het Hof heeft volgens Britz de kans laten liggen om de doelen die ten grondslag liggen aan de bescherming van gegevens en informatie, te concretiseren.[330] Naar de mening van Eifert maakt het niet uit of de nieuwe systemen bijzonder veel en bijzonder gevoelige gegevens verwerken. Informationele zelfbeschikking moet daar juist tegen beschermen. Eifert vindt de nadruk op integriteit van systemen ontoereikend, omdat de nadruk vooral technisch en instrumenteel is, in plaats van persoonlijkheidsgericht. De verwijzing naar de persoonlijkheid is volgens hem slechts indirect en instrumenteel. Het blindstaren op de integriteit van systemen kan de bescherming van andere grondrechten ondermijnen. Immers wanneer voldaan is aan het vereiste van integriteit kan er sprake zijn van toegang tot de gegevens.

Daarnaast beperkt het Hof de reikwijdte van het recht op informationele zelfbeschikking. Omvangrijke gegevensverzamelingen worden hier niet onder geschaard. Het is onduidelijk hoe deze deelrechten van het persoonlijkheidsrecht zich precies tot elkaar verhouden. Hoffmann-Riem, ten tijde van het oordeel rechter van het Constitutioneel Hof, geeft in reactie hierop aan dat het arrest niet moet worden gelezen als een omvattend betoog over het bereik van het recht op informationele zelfbeschikking.

Ter ondersteuning van het oordeel geeft de, destijds voorzitter van het Constitutioneel Hof, Hans Jürgen Papier, aan dat de technische mogelijkheden om informatie te verzamelen ten tijde van de Census-zaak (1983) helemaal niets voorstellen bij wat er anno 2008 allemaal mogelijk is.[331] Hoffmann-Riem schetst de veranderingen van gevaren en kansen door communicatietechnologieën.[332] Er zijn niet meer centrale opslaglocaties van gegevens, maar er is decentrale en globale opslag van en toegang tot gegevens. Veel van de huidige technologieën zijn van na 1983. Kutscha beaamt dat er door huidige informatiesystemen talrijke gegevens worden geproduceerd en achter de rug om van de gebruiker verzonden worden.[333] Dat is ook de reden voor het Hof om een nieuw grondrecht te formuleren. Hornung is het daarmee eens vanuit de gedachte dat het recht op informationele zelfbeschikking uitgaat van afzonderlijke gegevensverwerking, en niet van grootschalige systematische gegevensverwerking, die onvoldoende bescherming biedt voor de persoonlijkheid. Hoffman-Riem betoogt dat grondwettelijke bescherming van de persoon met betrekking tot technologische communicatie moet worden vertaald in bescherming door middel van de technologische infrastructuur en de functiemogelijkheden van de technologie.[334] Het nieuwe grondrecht is volgens hem nodig omdat bescherming van gegevens iets anders is dan bescherming van de systemen die gegevens verwerken. Toegang tot informatiesystemen wordt volgens hem slechts gedeeltelijk beperkt door het recht op informationele zelfbeschikking. Bescherming van de persoonlijkheid

330. Britz 2008, p. 413.
331. Ermert 2008.
332. Hoffmann-Riem 2008, p. 1010.
333. Kutscha 2012, p. 392.
334. Hoffmann-Riem 2008, p. 1011-1017.

vereist dat de gegevens binnen informatiesystemen niet in samenhang en zonder autorisatie door derden kunnen worden gebruikt. Dat is echter wel mogelijk door middel van infiltratie van informatiesystemen waartegen personen zich niet kunnen wapenen.

Het nieuwe grondrecht reguleert toegangsvrijheid, manipulatievrijheid en eenzijdig machtsgebruik of -misbruik. Hoffmann-Riem is wel zo realistisch dat de Staat de functiemogelijkheden van communicatie-infrastructuren slechts tot op zekere hoogte kan begrenzen, vanwege de mondiale reikwijdte van het net en de macht van de private partijen. Maar volgens hem kan de Staat wel gebruikmaken van de macht om het recht te bepalen en normen te stellen voor gedrag en controle op het net, door wettelijke maatregelen die invloed hebben op de configuratie van informatiesystemen, of die technologische gegevensbescherming en zelfbescherming door middel van versleuteling mogelijk maken. Op die manier kan de vertrouwelijkheid en integriteit van informatiesystemen gewaarborgd worden voor zover dat persoonlijkheidsrelevant is. Dat is afhankelijk van het al dan niet verwerken van persoonlijkheidsrelevante gegevens door systemen.

De bescherming van de persoonlijkheid eist dat er niet wordt ingegrepen in het kerndomein van het privéleven. Volgens sommige rechtswetenschappers levert dit nieuwe grondrecht daartoe extra bescherming ten opzichte van het recht op informationele zelfbeschikking.[335] Wieczorek betoogt dat een volledige bescherming van de persoonlijkheid niet alleen vraagt om bescherming van informatiesystemen en persoonsgegevens, maar ook bescherming van informatie.[336] Hoffmann-Riem geeft toe dat het Hof had kunnen kiezen voor een uitbreiding van het recht op informationele zelfbeschikking om online doorzoekingen te reguleren.[337] Hij betoogt dat dit niet is gebeurd, vanuit de grondwettelijke systematiek waarbij het persoonlijkheidsrecht telkens is uitgewerkt in deelrechten. Hij en zijn collega's komen tot het oordeel dat informatiesystemen noodzaken tot afzonderlijke grondwettelijke bescherming, die niet gebaseerd is op een fictie van persoonlijkheidsbescherming door middel van zelfbescherming, maar het verlangen naar bescherming van vertrouwen op de voorgrond stelt. Dat maakt het mogelijk om nieuwe eisen te stellen aan systemen. Het maakt het ook mogelijk om niet alleen vanuit deelconcepten de vertrouwelijkheid en integriteit van systemen aan de orde te stellen, maar vanuit een alomvattend concept.

Problematisch wordt daarmee wel de afgrenzing van het recht op informationele zelfbeschikking en het recht op vertrouwelijkheid en integriteit van informatiesystemen. Volgens Hoffmann-Riem moet het recht op informationele zelfbeschikking beschermen tegen gegevensverzamelingen en verdere gegevensverwerking zonder infiltratie van informatiesystemen en tegen de creatie van overeenkomstige machtigingen.[338] Het nieuwe grondrecht geldt wanneer er

335. Hoffmann-Riem 2008, p. 1009 e.v.
336. Wieczorek 2011.
337. Hoffmann-Riem 2008, p. 1009 e.v.
338. Hoffmann-Riem 2008, p. 1015.

sprake is van doorvoeren van gegevensverzamelingen door middel van infiltratie, gebruik en manipulatie van een complex informatiesysteem. Opvallend is dat Papier en Hoffman-Riem niet de Staat, maar marktpartijen als de grootste bedreiging zien voor die vrijheid.[339] Kutscha geeft ook aan dat een grondrecht op vertrouwelijkheid en integriteit van informatiesystemen alleen werkelijk bescherming kan bieden indien private partijen hierdoor ook worden gereguleerd.[340] Ro nagel en Schnabel leiden uit het nieuwe grondrecht dan ook consequenties af voor private rechtsverhoudingen en de verplichting van de wetgever voor overeenkomstige wetgeving.[341]

Het oordeel van het Hof geeft richtlijnen voor het online doorzoeken van informatiesystemen, en voor andere surveillancemethoden.[342] Mede daarom wordt het arrest beschouwd als zeer belangrijk voor de bescherming van privacy, bescherming van persoonsgegevens en informationele zelfbeschikking.
Uit het arrest blijkt niet hoe het nieuwe 'computer-grondrecht' precies moet worden afgegrensd ten opzichte van andere grondrechten. Het nieuwe grondrecht hoeft zich niet te beperken tot bescherming tegen heimelijke infiltratie. Ook beschermt dit het belang van de gebruikers dat de door de informatiesystemen verzamelde, verwerkte en opgeslagen gegevens vertrouwelijk blijven.[343] Het gaat daarbij niet alleen om online doorzoekingen van Staatsautoriteiten maar ook door private partijen, in het bijzonder Google of Facebook. Uit deze zaak kan als gevolg van de nieuwe technologische ontwikkelingen op het gebied van opsporing dus mogelijk een inperking van de reikwijdte van het recht op informationele zelfbeschikking worden gelezen door een nieuw 'recht op integriteit van systemen'.

4.4.4 Demonstratievrijheid

Na het '*Online-Durchsuchungen Urteil*' heeft het Constitutioneel Hof nog een aantal belangwekkende arresten gewezen met betrekking tot informationele zelfbeschikking en bescherming van de persoonlijkheid.
In 2009 oordeelt het Hof dat Beierse wetgeving strijdig is met de demonstratievrijheid.[344] Daarbij wijst het Hof onder meer op het filmen van alle demonstranten, waardoor mensen kunnen worden herkend, wat hen in problemen kan brengen, onder andere door het opleggen van boetes, en kan weerhouden van het demonstreren. In de Census-zaak wees het Hof er al op dat een inperking van het recht op informationele zelfbeschikking voor het ongewenste effect kan zorgen dat mensen risicomijdend gedrag gaan vertonen, met als gevolg dat mensen mogelijk niet opkomen voor hun rechten door demonstraties of anderszins.
Hier blijkt wederom dat het recht op informationele zelfbeschikking meer dan één toepassing heeft en dat de sociale en psychologische gevolgen van het niet

339. Ermert 2008; Hoffmann-Riem 2008, p. 1010, 1018.
340. Kutscha 2012, p. 392.
341. Roßnagel & Schnabel 2008, p. 3534.
342. Hornung & Schnabel 2009b, p. 116.
343. BVerfG 27 februari 2008, BVerfGE 120, 274 (314) (Online-Durchsuchungen).
344. BVerfG 17 februari 2009, BVerfGE 122, 342 (Bayerisches Versammlungsgesetz).

zelf kunnen beschikken over informatie, bijvoorbeeld videobeelden van jezelf tijdens een demonstratie, iets zijn wat de rechter in acht neemt bij het beoordelen van schendingen.

4.4.5 Dataretentiewetgeving

Het Hof oordeelt in 2010 over de gegevensretentiewetgeving in Duitsland, ter implementatie van Europese regelgeving.[345] Deze wetgeving roept heftige reacties op in Duitsland en scherpe kritiek van juristen, resulterend in 34.000 individuele klagers.[346] De advocaat-generaal bij het Europese Hof van Justitie, Kokott, en de Article 29 Working Party twijfelen of de gegevensretentie in overeenstemming is met Europese grondrechten als privacy.[347] Het idee om alle gegevens te bewaren is overigens niet nieuw. Enkele politici proberen dit al een tijd in te voeren, maar de Bundestag heeft dit verworpen, met als een van de belangrijkste argumenten dat het Constitutioneel Hof hier niet mee akkoord zou gaan. Daarnaast valt het onderscheid weg tussen verdachten en onschuldige burgers.[348] Oorspronkelijk is beoogd een EU Kaderrichtlijn vast te stellen voor gegevensretentie. Dit initiatief haalt het echter niet, en in plaats daarvan is een richtlijn vastgesteld. Sommige politici hebben mogelijk gedacht dat het Europees recht een mogelijkheid biedt om te ontsnappen aan het strenge onderzoek van het Duitse Hof, wat ijdele hoop bleek.

Richtlijn 2006/24/EC betreffende de opslag van gegevens, is door Duitsland omgezet in artikelen in de Telecommunicatiewet (*Telekommunikationsgesetz*) en het Wetboek van Strafvordering (*Strafprozessordnung*). Artikel 113a van de Telecommunicatiewet bepaalt dat publiek toegankelijke communicatiediensten uit voorzorg de taak hebben om al het gegevensverkeer op te slaan dat van belang is om te reconstrueren wie, wanneer, hoe lang, met wie en waarvandaan heeft gecommuniceerd. De inhoud van de communicatie, bijvoorbeeld de bezochte internetpagina's, dient niet opgeslagen te worden. Na de gegevens zes maanden opgeslagen te hebben, dienen de gegevens binnen één maand verwijderd te worden. Dit is nog een minimale implementatie van Richtlijn 2006/24/EC, aangezien twee jaar gegevensopslag is toegestaan. De gegevens mogen direct gebruikt worden voor de vervolging van serieuze strafbare feiten. Indirect mogen gegevens gebruikt worden voor de herkenning van IP-adressen, die al bekend zijn bij de autoriteiten, in het kader van strafvervolging.

Het recht op informationele zelfbeschikking is door de personen die tegen deze wettelijke regeling klagen bij het Constitutioneel Hof ingeroepen, naast artikel 10 GG dat het correspondentiegeheim beschermt. Het Hof geeft aan artikel 10 GG als een speciale bescherming van het recht op informationele zelfbeschik-

345. BVerfG 2 maart 2010, BVerfGE 125, 260 (Vorratsdatenspeicherung).
346. Hornung & Schnabel 2009b, p. 120.
347. Opinion of the Advocate General, 18 July 2007, C-275/06, Promusicae vs. Telefónica de España, para 82; Article 29 Gegevens Protection Working Party, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of gegevens generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, March 2006.
348. Hornung & Schnabel 2009b, p. 119.

king te zien, waardoor het algemene recht niet meer hoeft te worden ingeroepen. Het Hof oordeelt dat de Duitse implementatiewetgeving in strijd is met artikel 10 GG aangezien de rechterlijke controle en effectieve juridische remedies ontbreken ten aanzien van het opslaan en gebruik van gegevens, de transparantie van het opslaan en gebruik van gegevens ontbreekt, en het principe van proportionaliteit niet door de gegevensretentieregels wordt nageleefd. De gegevensretentiewetgeving is door het Hof wegens strijd met de Grondwet buiten werking gesteld in lijn met de hieronder uitgelegde '*So lange*'-jurisprudentie van het Constitutioneel Hof.
Het recht op informationele zelfbeschikking blijft dus ook haar functie als afweerrecht houden, naast haar andere toepassingen die meer betrekking hebben op zaken als keuzevrijheid en zelfontplooiing bij het omgaan met persoonlijke informatie.

4.4.6 De evolutie van het Constitutioneel Hof

In reactie op de jurisprudentie van het Constitutioneel Hof inzake bescherming van de persoonlijkheid betogen Hornung en Schnabel dat de positie van het Constitutioneel Hof radicaal maar consistent is. Zij constateren ook dat er een verdeling van taken is. Bij veiligheidswetten en -maatregelen kijkt het Hof naar de grondwettelijkheid hiervan. De politiek laat het afweten vanwege verschillende redenen.[349] Parlement en regering moeten ook aan de Grondwet voldoen maar vragen aan het Hof voor invoering van de regelgeving of het voldoet aan grondwettelijke eisen. Deze verdeling van taken bestempelen Hornung en Schnabel als gevaarlijk. Er is ook veel druk vanuit de politiek op de politieke beslissingen die het Constitutioneel Hof neemt, maar dat leidt nog niet tot een sterke aantasting van de bescherming van de persoonlijkheid en menselijke waardigheid.

4.5 CONCLUSIE DUITSLAND

In het Censusoordeel van 1983 heeft het Duitse Constitutioneel Hof het wenselijk geacht een halt toe te roepen aan ongebreidelde verzameling en gebruik van persoonlijke gegevens.[350] Daartoe heeft het Hof een recht op informationele zelfbeschikking geformuleerd als uitwerking van het sterk op waarden gefundeerde algemeen persoonlijkheidsrecht en het onderliggende recht op menselijke waardigheid.
Vervolgens is het recht op informationele zelfbeschikking op verschillende manieren uitgewerkt in Duitse wetgeving en jurisprudentie, waarvan de bescherming van persoonsgegevens als belangrijkste kan worden aangemerkt. Het recht op privacy is in de jurisprudentie ook afgeleid uit het algemeen persoonlijkheidsrecht en de menselijke waardigheid.[351] Gesteld kan worden dat bescherming van persoonsgegevens een domein is waar het recht op informationele zelfbeschikking en het recht op privacy elkaar raken. Over de exacte

349. Zie Hornung, Bendrath & Pfitzmann 2010, p. 145.
350. BVerfG 15 december 1983, BVerfGE, 65, 1 (43) (Volkszählung); Schwartz 1989, p. 688; zie ook J. Taeger, Die Volkszählung, 1983.
351. BVerfG 15 januari 1970, BVerfGE 27, 344 (Ehescheidungsakten).

relatie tussen informationele zelfbeschikking, privacy en bescherming van persoonsgegevens is veel discussie in de wetenschappelijke literatuur.

Zoals geconstateerd is in de wetenschappelijke literatuur tevens discussie over de wenselijkheid, mogelijkheid en interpretatie van een recht op informationele zelfbeschikking. Aangaande de wenselijkheid is er onenigheid over de mate waarin vrije informatieverzameling en -uitwisseling, en daarmee verscheidene grondrechten, mogen worden beperkt. Daarnaast is in de wetenschappelijke literatuur het gevaar genoemd dat het recht op informationele zelfbeschikking tot een vervreemdbaar eigendomsrecht verwordt, al wordt daar door anderen juist voor gepleit.[352] Tevens is er discussie over het bereik van informationele zelfbeschikking, in het bijzonder wat betreft de vraag of private partijen hier ook onder vallen.

Wat betreft de feitelijke levensvatbaarheid en daarmee effectiviteit van een recht op informationele zelfbeschikking, kan worden geconcludeerd dat de Duitse rechtspraak en wetgeving aantonen dat een recht op informationele zelfbeschikking een belangrijke rechtsstatelijke en beschermende rol kan spelen. Daarbij kan natuurlijk altijd worden ingebracht of dit recht in een effectieve vorm van bescherming heeft geresulteerd die niet al zonder een expliciete erkenning van dit recht had kunnen worden geboden. Het antwoord op deze laatste vraag kan zowel bevestigend als ontkennend zijn. Uitgaande van het persoonlijkheidsrecht en het funderende recht op menselijke waardigheid kan worden betoogd dat deze rechten op zich al de benodigde rechtsbescherming kunnen bieden. Evenwel heeft de Duitse rechter met opzet gekozen voor het preciseren van het persoonlijkheidsrecht in verschillende deelrechten, wat kan worden beschouwd als de erkenning van de noodzaak tot aanvullende bescherming op deze specifieke deelgebieden en een rechtsstatelijk antwoord op nieuwe maatschappelijke en technologische ontwikkelingen. De maatschappelijke en technologische ontwikkelingen ten aanzien van de mogelijkheden om gegevens te verzamelen en te gebruiken, zijn immers alleen maar verder gegaan. Volgens het Duitse Hof heeft dat de uitoefening van het recht op informationele zelfbeschikking zodanig bemoeilijkt dat het onderliggende persoonlijkheidsrecht en de funderende menselijke waardigheid niet voldoende kunnen worden genoten. In antwoord daarop heeft het Hof het 'computergrondrecht' geformuleerd.[353] Over de mogelijkheid en wenselijkheid van dit recht is een stevige discussie ontstaan. In de wetenschappelijke literatuur gaan sommigen mee met de argumentatie van het Hof dat het in het huidige maatschappelijke en technologische klimaat onmogelijk is vol te houden dat de persoon de beschikking heeft over de op hem betrekking hebbende informatie en überhaupt in staat is daarover de beschikking te hebben.[354] Hier lijkt zich de nadruk op zelfbeschikking te wreken. In lijn met deze redenering is de conclusie dat grondwettelijke bescherming vereist is via een computer-grondrecht.

352. Rouvroy en Poullet; Dommering 2010, p. 83-99.
353. BVerfG 27 februari 2008, BVerfGE 120, 274 (Online-Durchsuchungen).
354. Hornung & Schnabel 2009b; Hoffmann-Riem 2008; Wieczorek 2011.

Een totaal andere conclusie is dat erkend en geaccepteerd moet worden dat in de huidige samenleving nu eenmaal veel meer gegevens over een persoon bekend zijn dan enkele decennia geleden. Anderzijds keren sommigen zich in de wetenschappelijke literatuur tegen de beperking van de werking van het recht op informationele zelfbeschikking.[355] Dit vanuit de idee dat informationele zelfbeschikking, als open concept, wel degelijk bescherming tegen het gebruik van informatiesystemen zelf omvat en zou moeten omvatten.[356] Het is volgens hen aan de rechter om nieuwe maatschappelijke en technologische fenomenen onder het bereik van informationele zelfbeschikking te brengen.

De literatuur onderscheidt in het algemeen persoonlijkheidsrecht drie elementen: zelfbeschikking, zelfexpressie en zelfbescherming.[357] Om op die grondrechten terug te vallen dient afdoende rechtsstatelijke bescherming te worden geboden. De Duitse rechter kiest ervoor om daarbij opnieuw nieuwe grondrechten te formuleren als het computer-grondrecht. Deze systematische aanpak heeft het voordeel van een grote mate van rechtszekerheid, maar kan tekortschieten in flexibiliteit om op nieuwe ontwikkelingen te reageren.

Specifiek ten aanzien van het recht op informationele zelfbeschikking in Duitsland kan alvast ten dele een antwoord worden gegeven op onderstaande eerste algemene onderzoeksvraag van deze dissertatie.

I **Is informationele zelfbeschikking mogelijk en wenselijk, in hoeverre en met welke be-perkingen? Kan en moet daarbij onderscheid worden gemaakt naar typen personen?**

Met betrekking tot deze onderzoeksvraag kan voor Duitsland worden geconcludeerd dat het recht op informationele zelfbeschikking als facet van het algemeen persoonlijkheidsrecht en recht op menselijke waardigheid mogelijk is en wenselijk binnen het Duitse rechtsstelsel, maar onvoldoende rechtsbescherming biedt, omdat:

1. het recht op informationele zelfbeschikking onvoldoende het onderliggende algemeen persoonlijkheidsrecht en de funderende menselijke waardigheid kan beschermen tegen de snelle maatschappelijke en technologische ontwikkelingen. In het huidige maatschappelijke en technologische klimaat is onmogelijk vol te houden dat de persoon de beschikking heeft over de op hem betrekking hebbende informatie en überhaupt in staat is daarover de beschikking te hebben. Vandaar dat het Hof het 'computer-grondrecht' heeft geformuleerd dat beoogt bescherming te bieden tegen het gebruik van informatiesystemen;

2. degenen die vinden dat maatschappelijke en technologische ontwikkelingen wel onder informationele zelfbeschikking te brengen zijn, maar dit aan de

355. Kutscha 2012; Lepsius 2008, p. 31; Britz 2008, p. 413; Eifert 2008.
356. Gola & Schomerus 2012; Hoffmann-Riem 2008, p. 1022.
357. Pieroth & Schlink 2006.

rechter willen overlaten om op die manier flexibel en responsief te blijven, impliciet ook de vraag stellen of aan het begrip 'zelfbeschikking' inhoud kan worden gegeven.

Anders dan in de hierna te bespreken hoofdstukken over Europa en Nederland kent de Duitse Grondwet geen algemeen recht op privacy. Aanknopingspunten voor de bescherming hiervan worden gevonden in het recht op informationele zelfbeschikking, menselijke waardigheid en het algemeen persoonlijkheidsrecht.

5. *Privacy en gegevensbescherming in Europa*

5.1 INLEIDING

Op Europees niveau wordt het begrip informationele zelfbeschikking niet zo expliciet gehanteerd als in het vorige hoofdstuk over Duitsland. Op Europees niveau kennen we het Europees Hof voor de Rechten van de Mens (EHRM) en het Hof van Justitie van de EU (HvJ EU). Hoewel in het EVRM geen expliciet recht op informationele zelfbeschikking is opgenomen kan uit de rechtspraak van het EHRM impliciet een recht op informationele zelfbeschikking worden afgeleid.[358] De rechtspraak van het EHRM gaat regelmatig over de bescherming van de persoonlijke levenssfeer in medische situaties.[359]

Het expliciete recht op informationele zelfbeschikking in Duitsland heeft een relatie met de Europese begrippen 'privacy' en 'bescherming van persoonsgegevens'. Allereerst komt het begrip 'privacy' aan bod en daarna het begrip 'bescherming van persoonsgegevens'. Gevolgd door de rechtspraak van het EHRM en het HvJ-EU.

5.2 HET BEGRIP PRIVACY

Als uitwerking van het begrip informationele zelfbeschikking komt eerst het begrip privacy aan de orde. Meer precies het recht op respect voor het privéleven.

In het beroemde artikel van Warren en Brandeis uit 1890 is privacy als een afweerrecht geformuleerd: '*the right to be let alone*'.

> *"In very early times, the law gave a remedy only for physical interference with life and property. […] Gradually the scope of these rights broadened; and now the right to life has come to mean the right to enjoy life – the right to be let alone."*[360]

Het Amerikaanse privacyrecht ontwikkelde zich in reactie op de uitvinding van de draagbare fotocamera. Overigens speelde ook in Nederland de draagbare fotocamera een belangrijke rol in de eerste literatuur waarin aandacht werd

358. Zie dissenting opinion van rechter Pikis in EHRM 22 april 1993, *Modinos t. Cyprus*, nr. 15070/89 en expliciet in dissenting opinion Petitti in EHRM 2 augustus 1984, *Malone t. het VK*, nr. 8691/79, *NJ* 1988, 534.
359. EHRM 29 april 2002, *Pretty t. het VK*, nr. 2346/02, EHRM 29 april 2002, *Pretty t. het VK*, nr. 2346/02, EHRM 7 maart 2006, *Evans t. het VK*, nr. 6339/05, *NJCM-Bulletin* 2006, p. 863 (m.nt. C.J. Forder & J. Whittingham), *GJ* 2006, 43 (m.nt. A.C. Hendriks), *EHRC* 2006, 47 (m.nt. E. Brems), § 57, EHRM 20 maart 2007, *Tysia c t. Polen*, nr. 5410/03, *NJCM-Bulletin* 2007, p. 497 (m.nt. A.C. Hendriks), *EHRC* 2007, 70 (m.nt. H.L. Janssen), § 107.
360. S.D. Warren, L.D. Brandeis, 'The Right to Privacy', Harvard Law Review, Boston 1890-5, p.193.

besteed aan de bescherming van de persoonlijke levenssfeer, zoals verder is uitgewerkt in paragraaf 6.2.1.

Rodota geeft aan dat onder invloed van de definitie van Warren en Brandeis privacy ook is opgevat als een instrument om minderheden en afwijkende opvattingen te beschermen. Dat is verbonden aan de vrijheid van meningsuiting en het recht op vrije ontwikkeling van de persoonlijkheid. In de economische duiding van het privacyrecht door Posner in de jaren tachtig van de twintigste eeuw kan de benadering van negatieve bescherming nog steeds worden onderscheiden.[361] Het economische privacyrecht wordt door hem gefundeerd op het economisch belang om als persoon feiten over jezelf al dan niet aan de buitenwereld te tonen. Deze benadering, waarbij Dommering zich heeft aangesloten, wordt hieronder uitgewerkt bij de bespreking van het begrip 'bescherming van persoonsgegevens'.[362]

Het concept van privacy heeft zich verder ontwikkeld, waarbij een positievere vorm van bescherming wordt nagestreefd, met daaraan verbonden verplichtingen voor de Staat en private partijen. Dit is te herkennen in de definitie van privacy door Friedman:

> *"The protection of life choices against any form of public control and social stigma".*[363]

Rosen heeft privacy eveneens ruim geformuleerd:

> *"Vindication of the boundaries protecting each person's right not to be simplified, objectified, and evaluated out of context".*[364]

Rodota formuleert privacy in relatie tot het controleren van informatie, wat van belang is in de context van informationele zelfbeschikking:

> *"The right to keep control over one's own information and determine the manner of building up one's own private sphere".*[365]

Solove relateert informatievraagstukken ook nadrukkelijk aan zijn concept van privacy, waarbij hij vier categorieën van privacy onderscheidt: informatieverzameling, -verwerking, -verspreiding, en binnendringen in de privésfeer.[366] Allan Westin formuleerde in het klassiek geworden '*Privacy and freedom*' de kern van privacy als volgt:

> *"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. (…) Privacy is the voluntary and temporary withdrawal of a person from the general society*

361. Posner 1983, p. 231 e.v.
362. Dommering, in: Prins 2010, p. 83-99.
363. Friedman 1990, p.184.
364. Rosen 2000, p. 20.
365. Rodotà 1995, p.122.
366. Solove, 2007, p. 745-772.

through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in condition of anonymity or reserve."[367]

Het begrip '*claim*' in de privacydefinitie van Westin sluit aan bij het woord 'vermogen' in mijn definitie van informationele zelfbeschikking. Bij 'vermogen' gaat het om de mate waarin de claim herkend wordt. Privacy als een 'claim' is iets wat meegewogen dient te worden, afhankelijk van de omstandigheden van het geval.

Ten slotte kan bij Rigaux een zeer ruime definitie van privacy worden gevonden:

"The right to freely choose one's life".[368]

Tussen Westin en Rigaux is een botsing zichtbaar tussen de Amerikaanse en Europees-Franse cultuur. De Amerikaan Westin beperkt zich tot een claim en de Europese Fransman Rigaux maakt er een breed recht van.

De definitie van privacy krijgt bij Rigaux een heel grote reikwijdte. Hier kan worden geconcludeerd dat privacy zowel een 'negatieve' component kent, waarbij afscherming van de eigen privésfeer voorop staat, als een 'positieve' component, waarbij het gaat om het hebben van controle over eigen informatie en het bepalen hoe de privésfeer kan worden opgebouwd.[369]

In juridische zin werd het concept van een recht op privacy na de Tweede Wereldoorlog als eerste – in een nog wat zwakke vorm – neergelegd in artikel 12 van de Universele Verklaring van de Rechten van de Mens op grond waarvan '*no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence*'.[370] Een meer krachtige bescherming volgde in artikel 8 EVRM[371], op grond waarvan iedereen het recht heeft op bescherming van zijn privé- en familieleven, zijn huis en correspondentie en geen interventie van publieke autoriteiten met betrekking tot het uitoefenen van zijn rechten is toegestaan, behalve dan wanneer dit in overeenstemming is met de wet en noodzakelijk is in een democratische samenleving vanwege zwaarwegende belangen.

Artikel 8 EVRM luidt:

"1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."

367. Westin, 1967, p. 7.
368. Rigaux, 1990, 167.
369. Rodota, in: Gutwirth 2009. p. 79-80.
370. Universele Verklaring van de Rechten van de Mens, 1948, GA Res, 217 A (III).
371. Europese Verklaring van de Rechten van de Mens 1950, ETS 5.

Het recht op privéleven, zoals dat in het eerste lid is geformuleerd, betreft informatie van min of meer gevoelige aard. Vandaar dat inbreuken op dit privacyrecht alleen onder de condities van het tweede lid zijn toegestaan. Artikel 8 EVRM beschermt privacy en daarmee de gevoelige persoonsgegevens die direct raken aan het privéleven. Het recht op privacy lijkt alleen om zogenoemde 'gevoelige gegevens' te gaan. Daarmee wordt het onderscheid tussen het recht op privacy en het recht op bescherming van persoonsgegevens duidelijk gemaakt.[372]

De verwijzing naar 'woning' en 'correspondentie' bouwde voort op de constitutionele traditie in vele landen van de wereld. De focus op 'privacy' en 'privéleven' was nieuw en een duidelijke reactie op de Tweede Wereld Oorlog.[373]

In de Europese rechtsorde hebben privacybescherming en de bescherming van persoonsgegevens een zelfstandig te benoemen karakter. Dit komt het duidelijkst naar voren in het Grondrechtenhandvest waarin naast het recht op eerbiediging van het privéleven, het familie- en gezinsleven, de woning en de communicatie (artikel 7) een apart recht is opgenomen voor de bescherming van persoonsgegevens (artikel 8).[374] Zie voor een verder uitgewerkte bespreking van het onderscheid tussen privacy en bescherming van persoonsgegevens paragraaf 5.3.[375]

Nissenbaum[376] bekritiseert de dominante, juridische denkwijze om het recht op privacy te zien als een recht op controle over informatie en het recht op geheimhouding. Deze definitie van privacy is volgens Nissenbaum te grofmazig. Het betekent dat ieder verlies aan controle een schending van de privacy is. Zo'n rigide definitie van privacy leidt tot een recht dat niet te verdedigen valt, omdat er alleen maar uitzonderingen op bestaan. Bovendien wordt privacy dan gereduceerd tot een individuele aangelegenheid, terwijl privacy ook gaat over anderen. Een van de centrale stellingen van Nissenbaum is dat mensen een privacyschending kunnen ervaren als partijen bij het verwerken van informatie normen overschrijden die binnen een specifieke context aanvaard zijn. Niet omdat mensen het gevoel hebben dat ze de controle kwijtraken of de geheimhouding wordt geschonden. Bij contextuele integriteit wordt het doel van een bepaalde context sociaal geconstrueerd. Een arts mag bijvoorbeeld niet zonder meer bepalen dat hij patiënteninformatie gaat gebruiken voor eigen onderzoek.

Een andere stelling van Nissenbaum, evenals van Moerel en Prins[377], is dat ten onrechte de handhavingsopdracht voor privacy momenteel primair bij indivi-

372. De Hert & Gutwirth 2009, p. 8-10; Hustinx 2005.
373. Hustinx, 2017, p.126.
374. Zie over de aparte opname van het recht op bescherming van persoonsgegevens in het Grondrechtenhandvest ook Blok, 2001.
375. Zie Hustinx, 1999 met drie concepten in het licht van ICT in de zorg:privacy, gegevensbescherming en informationele zelfbeschikking. Zie ook de weergave van de discussie die naar aanleiding van dit preadvies in Ploem, p. 301-305. Zie ook Hustinx, 2013 en 2017. En verder: Kranenborg & Verhey 2011, p. 2; Nissenbaum 2004; Post 2000.
376. Nissenbaum 2010.
377. Moerel & Prins 2016.

duen ligt. Vanuit het perspectief van informationele zelfbeschikking is deze stellingname zeer relevant, omdat informationele zelfbeschikking over het vermogen van een persoon gaat om in beginsel zelf te bepalen in hoeverre persoonsgegevens worden gebruikt en verder bekendgemaakt, met het oog op een zelfbepaald leven. In hoofdstuk 1 kwam het begrip 'doenvermogen'[378] al aan de orde en in hoofdstuk 2 de verschillende 'typen personen' en de complexe maatschappelijke en technologische ontwikkelingen waar vele personen geen vat op hebben. Ook bij de bescherming van persoonsgegevens in de AVG zullen we zien dat de handhavingsopdracht (te) veel bij personen wordt gelegd. Deze verantwoordelijkheid zou volgens Nissenbaum moeten worden verschoven naar verantwoordelijken door hun verwerkingen op basis van *privacy-by-design* in te richten.[379]

5.3 BESCHERMING VAN PERSOONSGEGEVENS

5.3.1 Overeenkomsten en verschillen met privacy

In het begin van de jaren zeventig constateert de Raad van Europa dat artikel 8 EVRM een aantal tekortkomingen heeft in het licht van nieuwe technologische en maatschappelijke ontwikkelingen.[380] Dit geldt in het bijzonder vanuit het perspectief van het groeiende gebruik van informatietechnologie.[381] Deze tekortkomingen zijn: de onzekerheid over de reikwijdte van 'privéleven', de nadruk op bescherming tegen inbreuk door 'publieke autoriteiten' en het gebrek aan een meer pro-actieve benadering, ook vanuit het oogpunt van mogelijk misbruik van persoonsgegevens door bedrijven en andere relevante organisaties in de private sector.[382] Deze conclusie leidt uiteindelijk tot het *Data Protectie Verdrag*. Dit is ook wel bekend als Verdrag 108, of het Verdrag van Straatsburg.[383] Het doel van dit verdrag was om alle personen binnen Europa te beschermen met respect voor hun fundamentele rechten en vrijheden met betrekking tot de automatische verwerking van persoonsgegevens. Persoonsgegevens werden gedefinieerd als 'iedere informatie in relatie tot een geïdentificeerde of identificeerbare persoon'.

Dit betekent dat 'bescherming van persoonsgegevens' breder is dan 'privacy', omdat het ook betrekking heeft op alle overige rechten en vrijheden en op alle soorten gegevens (ook 'gewone' persoonsgegevens en persoonsgegevens in het private domein) ongeacht hun relatie met privacy. Tegelijkertijd is 'bescherming van persoonsgegevens' ook een beperkter begrip dan privacy, omdat het betrekking heeft op het verwerken van persoonlijke gegevens en niet op andere aspecten van privacy (zoals ruimtelijke en relationele privacy).[384]

378. WRR, 2017.
379. Nissenbaum (2011)
380. Explanatory Report to Convention 108 (see note 9) at par. 4.
381. Zie Hustinx, 2017, p. 126.
382. In deze dissertatie doemt de vraag op of deze tekortkomingen ook gelden voor de huidige wet- en regelgeving in het licht van de opkomst van bijvoorbeeld persoonlijke gezondheidsomgevingen.
383. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981, ETS 108.
384. Hustinx, 2017, p.127.

De overeenkomsten en verschillen tussen het recht op privacy – preciezer 'recht op privéleven' – en het recht op bescherming van persoonsgegevens zijn volgens diverse auteurs van belang.[385] Privacy en de bescherming van persoonsgegevens zijn beide een expressie van een universeel idee met ethische dimensies: autonomie en menselijke waardigheid.
Er zijn ook cruciale verschillen. Het concept 'bescherming van persoonsgegevens' is ontwikkeld om te voorzien in een structurele, juridische bescherming van personen tegen het onzorgvuldig gebruiken van informatietechnologie bij de verwerking van persoonsgegevens, ongeacht of dit past in de scope van het respecteren van het privéleven. Bij de bescherming van persoonsgegevens gaat het om een set van waarborgen – in essentie een systeem van checks en balances bestaande uit voorwaarden, individuele rechten en onafhankelijk toezicht – voor alle persoonsgegevens, gevoelig of ongevoelig voor het privéleven. Gegevensbescherming geeft een positieve bescherming ten aanzien van alle vormen en soorten van gegevens. Het is volgens Rodota in feite het eindpunt van een lang proces van ontwikkeling van het concept van privacy. Van een recht om alleen gelaten te worden tot het recht om controle te hebben over de eigen informatie en te bepalen hoe de privésfeer kan worden opgebouwd. Hier ziet Rodota in bescherming van persoonsgegevens als het ware een nieuwe, positieve formulering van het recht op privacy.[386]

Vanuit het Europese perspectief van de bescherming van persoonsgegevens komen hierna het al even genoemde Verdrag van Straatsburg, de OESO-richtlijnen, het Handvest en de AVG aan de orde.

5.3.2 Verdrag van Straatsburg

In 1981 is het 'Verdrag van Straatsburg', oftewel het Verdrag voor Gegevensbescherming van de Raad van Europa (Conventie 108) afgesloten. Dit is een intergouvernementele overeenkomst betreffende de geautomatiseerde gegevensverwerking omtrent personen.
Het is een relevant verdrag vanwege de acht daarin opgenomen beginselen. Deze acht beginselen zijn in twee groepen te verdelen.[387] De eerste vier betreffen voorwaarden waaronder persoonsgegevens verwerkt mogen worden. De laatste vier beginselen betreffen de verplichtingen van de voor gegevensverwerking verantwoordelijken en de rechten van individuen. Het gaat om de volgende acht beginselen:

385. De Hert & Gutwirth 2009, p. 8-10; Hustinx 2005 en 2017.
386. Rodota, 2009, p. 79-80.
387. Berkvens & Prins 2007, p.12.

Tabel 2: Beginselen Verdrag van Straatsburg

Beginselen	
1. Collection Limitation Principle; 2. Gegevens Quality Principle; 3. Purpose Specification Principle; 4. Use limitation Principle;	Voorwaarden waaronder persoonsgegevens verwerkt mogen worden
5. Security Safeguards Principle; 6. Openess Principle; 7. Individual Participation Principle; 8. Accountability Principle.	Verplichtingen van de voor gegevensverwerking verantwoordelijken en de rechten van individuen

Het doel van het Verdrag is volgens artikel 1 om ieder individu te beschermen, ongeacht diens nationaliteit of woonplaats, met respect voor zijn rechten en fundamentele vrijheden, en in het bijzonder zijn recht op privacy, met betrekking tot geautomatiseerde verwerking van bestanden met persoonsgegevens en geautomatiseerde verwerking van persoonsgegevens in de publieke en private sector.

Het Verdrag markeert een verschuiving naar het verwerken van alle soorten persoonsgegevens, ongeacht het karakter daarvan of de sector waarin zij verwerkt zijn. Zo bepaalt artikel 3, lid 1 dat het Verdrag zowel betrekking heeft op verwerking van persoonsgegevens door de overheid als door private partijen. Artikel 3, lid 2 geeft de mogelijkheid aan lidstaten om de werking van het Verdrag te beperken onder bepaalde voorwaarden. Bepaalde categorieën gegevens kunnen daardoor worden uitgesloten van de werking van het Verdrag. Het is echter ook mogelijk om de werking van het Verdrag te verruimen naar niet-natuurlijke personen en naar ongeautomatiseerde verwerking van persoonsgegevens.

In hoofdstuk 2 van het Verdrag van Straatsburg uit 1981 wordt een onderscheid gemaakt tussen 'gewone persoonsgegevens en een speciale categorie voor gevoelige persoonsgegevens, de gegevens waar onder andere artikel 8 EVRM op doelt. In artikel 6 wordt het verboden om speciale categorieën (gevoelige) gegevens te verwerken, tenzij er voldoende waarborgen in het nationale recht aanwezig zijn. Dit zijn bijvoorbeeld gegevens over etnische afkomst, politieke of religieuze achtergrond, gezondheidstoestand, seksueel gedrag of strafrechtelijke geschiedenis.

5.3.3 OESO-richtlijnen

Zowel het concept van de bescherming van persoonsgegevens als het recht op de bescherming van het privéleven (privacy) moeten worden onderscheiden van het recht op informationele zelfbeschikking, met een sterke nadruk op de toestemming van de persoon als datasubject aan de ene kant en de richtlijnen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO)

gebaseerd op de notie van risico en de veronderstelling dat alle verwerkingen van persoonsgegevens in principe legitiem zijn, aan de andere kant.[388]

De OESO die ook een aantal niet-Europese lidstaten heeft, ziet evenals de Raad van Europa de spanning onder ogen tussen het vrije verkeer van persoonsgegevens en de bescherming van de privacy. Een paar maanden voordat het Verdrag van Straatsburg werd vastgesteld stelde de OESO richtlijnen ter Bescherming van de Privacy en het Grensoverschrijdende Persoonsgegevensverkeer vast.[389] Hoewel de OESO-richtlijnen in tegenstelling tot het Verdrag van Straatsburg niet bindend zijn, hebben deze richtlijnen grote invloed, in het bijzonder bij landen buiten Europa, zoals de Verenigde Staten, Canada, Australië en Japan. De richtlijnen bevatten een set van basis-principes die in nauwe afstemming met het Verdrag van Straatsburg tot stand zijn gekomen en grotendeels consistent zijn met de principes van dit Verdrag. Er is echter ook een subtiel, maar belangrijk verschil. De OESO-richtlijnen zijn beperkt tot persoonsgegevens die een risico vormen voor de privacy en de individuele vrijheden. Deze op risico's gebaseerde benadering is niet verenigbaar met de op fundamentele mensenrechten gebaseerde benadering van de Raad van Europa en daarna de Europese Unie. Bovendien ontbreken het doelbindingsvereiste en de noodzakelijke rechtmatige grondslag om persoonsgegevens te mogen verwerken in de OESO-richtlijnen. In wereldwijde discussies over privacy en bescherming van persoonsgegevens zijn dit relevante verschillen.[390]

5.3.4 Richtlijn 95/46/EG

Richtlijn 95/46/EG[391] is inmiddels vervangen door de AVG.[392] Vandaar dat deze richtlijn hier slechts kort aan de orde komt. Deze richtlijn is de basis van de jurisprudentie van het Europees Hof van Justitie (HvJ-EU) in de periode voorafgaand aan de AVG. En de richtlijn was ook de basis voor de Wbp die in Nederland eveneens vervangen is door de AVG. Richtlijn 95/46/EG was een reactie op het Verdrag van Straatsburg. De Europese Commissie was bezorgd over het gebrek aan consistentie tussen de verschillende wetten die de lidstaten van Europa op basis van het Verdrag tot stand hadden gebracht en de bijbehorende verschillen in rechtsbescherming van personen. Het belangrijkste doel van deze richtlijn was dan ook het harmoniseren van de bescherming van persoonsgegevens in de Lidstaten op een hoog niveau. Tegelijkertijd formuleerde de richtlijn open standaarden, waardoor er geen volledig identieke en consistente wetgeving ontstond.[393]

388. Hustinx, 2017, p.130.
389. Recommendation of the Council (23 September 1980), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Gegevens, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
390. Hustinx, 2017, p.131.
391. 'Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van gegevens.' PbEG 1995 L 281/31.
392. Verordening (EU) 2016/679 (AVG) van 24 mei 2016.
393. Hustinx, 2017, p.132.

De richtlijn volgde de basis-principes van het Verdrag van Straatsburg en voegde daar criteria voor gerechtvaardigde gegevensverwerking aan toe. De richtlijn gaf ook aan onder welke voorwaarden bijzondere gegevens (zoals gezondheidsgegevens) verwerkt mochten worden. Het uitgangspunt was: Verboden, tenzij. Een ander nieuw kenmerk van de richtlijn was dat de verantwoordelijke voor de gegevensverwerking aan de betrokken persoon in beginsel adequate informatie moest geven. Ook werden in de richtlijn bepalingen opgenomen over de toezichthouders die ieder land moest aanstellen en de samenwerking tussen die toezichthouders binnen Europa in de zogenoemde 'Artikel 29 werkgroep' en een Europese Dataprotectie Toezichthouder (EDPS).

5.3.5 EU-Handvest

De EU heeft de rol van de Raad van Europa overgenomen waar het gaat om het verder ontwikkelen van het concept van de bescherming van persoonsgegevens. In dat opzicht zijn er twee trends zichtbaar. In de eerste plaats zijn het recht op privacy en het recht op gegevensbescherming beiden versterkt. In de tweede plaats de trend wordt om consistentere toepassing van deze rechten binnen de EU te bevorderen. Beide trends zijn gericht op meer consistente bescherming van deze rechten in de praktijk en minder diversiteit van deze bescherming in de verschillende lidstaten. De toenemende impact van het EU-Handvest, zowel in de rechtspraak als de wetgeving, is in lijn met deze langetermijntrend.
Het onderscheid tussen 'privacy' en 'bescherming van persoonsgegevens' is ook relevant voor het EU-Handvest.

Hiervoor kwam al aan de orde dat in het Handvest van de Grondrechten van de Europese Unie ook een expliciet onderscheid gemaakt wordt tussen de bescherming van het privéleven (artikel 7) en de bescherming van persoonsgegevens (artikel 8). Artikel 7 over de bescherming van het recht op een privéleven is een voorbeeld van een klassiek fundamenteel recht, waar slechts onder strikte voorwaarden van kan worden afgeweken. Artikel 8 over de bescherming van persoonsgegevens volgt het Verdrag van Straatsburg, de Europese richtlijn 95/46/EG en nu de AVG, door te voorzien in een systeem van meer proactieve bescherming. Volgens Rodota is de codificatie van de bescherming van persoonsgegevens in het Handvest EU de culminatie van de scheiding van privacy en gegevensbescherming.[394]

In de rechtspraak toont het Hof van Justitie een tendens om de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie gecombineerd te lezen. Terecht merkt Hustinx op dat dit geen recht doet aan de fundamentele verschillen tussen beide rechten.[395]

Het Handvest van de Grondrechten van de Europese Unie dateert van 2000. Dit Handvest is bindende Europese (grond)wetgeving via artikel 6 EU-verdrag. In artikel 1 Handvest wordt het recht op menselijke waardigheid vastgelegd. De

394. Rodota 2009.
395. Hustinx, 2017, 172.

menselijke waardigheid is onschendbaar en moet worden geëerbiedigd en beschermd ingevolge artikel 1. Op de notie van menselijke waardigheid is in Duitsland het algemene persoonlijkheidsrecht, en het daaruit voortvloeiende recht op informationele zelfbeschikking gefundeerd.
Daarnaast gaat het Handvest ten aanzien van gegevensbescherming dus verder dan andere verdragen, door zowel het recht op privacy (artikel 7) als het recht op bescherming van persoonsgegevens (artikel 8) vast te leggen.

> *"Artikel 7 Eerbiediging van het privé-leven en het familie- en gezinsleven*
> *Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.*
>
> *Artikel 8 Bescherming van persoonsgegevens*
> 1. *Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.*
> 2. *Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.*
>   *Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.*
> 3. *Een onafhankelijke autoriteit ziet toe op de naleving van deze regels."*

Artikel 52 Handvest geeft aan dat de rechten die in het Handvest zijn vastgelegd conform het Unieverdrag en het EVRM moeten worden uitgelegd, al is een ruimere bescherming van het Handvest wel mogelijk. Dommering ziet in deze bepaling een aanwijzing dat artikel 7 en 8 Handvest in feite twee aspecten (privacy en gegevensbeschermingrecht) van hetzelfde zelfbeschikkingsrecht (over de binnenkant en buitenkant van het privéleven) van artikel 8 EVRM zijn.[396] De Hert en Gutwirth zien artikel 8 Handvest echter als een nieuw recht op gegevensbescherming dat verder gaat dan andere verdragen en ook de meeste nationale wetgeving, in het bijzonder vergeleken met het recht op privacy.[397] Reikwijdte, doelen en inhoud verschillen volgens hen tussen het recht op gegevensbescherming en op privacy. Dit blijkt volgens De Hert en Gutwirth ook uit de jurisprudentie van het EHRM ten aanzien van artikel 8 EVRM. Rodota sluit zich aan bij deze opvatting. Hij geeft aan dat het Handvest de scheiding tussen privacy en gegevensbescherming als het ware bezegelt.[398] Volgens Rodota beschermt artikel 8 Handvest het 'elektronische lichaam', en is het in die zin verbonden met artikel 1 Handvest waarin de menselijke waardigheid wordt beschermd, en met de preambule waarin de Europese Unie de mens centraal wil stellen bij zijn activiteiten.[399] Het grondrecht op gegevensbescherming draagt volgens hem bij aan de constitutionalisering van de persoon. Gegevensbescherming is volgens Rodota een essentieel middel voor vrije ontwikkeling van de persoonlijkheid geworden.

Daarnaast gaat het Handvest verder, door gegevensbescherming ook van toepassing te verklaren op persoonlijke gegevens in privérelaties en in de private sector. De Hert en Gutwirth geven echter wel aan dat het te bezien valt of de

396. Dommering 2010.
397. Zie De Hert & Gutwirth 2009, p. 6-8.
398. Rodota 2009.
399. Rodota 2009.

rechters nu ook daadwerkelijk verdergaande bescherming zullen bieden naar aanleiding van deze codificatie van de bescherming van persoonsgegevens.

Wat betreft de tekst van artikel 8 Handvest kan er volgens Rouvroy en Poullet kritiek worden geuit op de formulering van het tweede lid, waarin wordt gesuggereerd dat toestemming voldoende is als legitieme grond voor elke vorm van verwerking.[400] Toestemming wordt op elektronische wijze vaak verworven door simpele interactie met netwerken. De eis van toestemming wordt door slim gebruik van technologieën uitgehold. Deze manier van omgaan met gegevensbescherming kan worden gerelateerd aan een opvatting van persoonlijke gegevens als zijnde vervreemdbaar eigendomsrecht dat kan worden verhandeld op de markt.[401]
Deze kritiek van Rouvroy en Poullet op toestemming als grondslag om persoonlijke gegevens te verhandelen, komt overeen met het eerder genoemde pleidooi van Jacobs[402] om in lijn met het bestaande verbod op het verhandelen van 'eigen' organen ook het commercieel exploiteren van 'eigen' medische gegevens te gaan verbieden.

Door het Verdrag van Lissabon[403], dat 1 december 2009 inwerking trad, kreeg het Handvest dezelfde juridische status als de verdragen in het Verdrag betreffende de werking van de Europese Unie (hierna: VwEU)[404].
De hierna te behandelen Algemene verordening gegevensbescherming (AVG), vindt zijn juridische grondslag in artikel 16, tweede lid VwEU. Hijmans laat zien dat de uitputtende formulering van artikel 16 VwEU geen ruimte laat voor autonome nationale wetgeving.[405]
Daarnaast veranderde door het Verdrag van Lissabon de institutionele structuur van de Europese Unie. Voor de totstandkoming van de AVG betekende dit dat niet langer alleen de Raad van Europa bepalend was, maar de Raad en het Europees Parlement gezamenlijk.

5.3.6 AVG

De AVG heeft 25 mei 2018 de Europese richtlijn 95/46/EG vervangen.[406]
De materiele scope van de AVG verschilt niet veel van de richtlijn. Het gaat evenals de richtlijn over de bescherming van persoonsgegevens en is eveneens in zowel de private als de publieke sector van toepassing. Het is voor iedereen zoeken naar hoe de nieuwe regels van de AVG in de praktijk dienen te worden

400. Rouvroy en Poullet 2009, p. 50.
401. Rouvroy en Poullet 2009, p. 72.
402. Jacobs, 2015.
403. http://www.minbuza.nl/ecer/eu-essentieel/verdragsteksten/6.-verdrag-van-lissabon.
404. Hustinx, 2017, p.151.
405. Zie Hijmans, 2016, 4.2, 4.3 en 6.2. Zie ook Hijmans 2018 en diens constatering die in paragraaf 6.2.1 van deze dissertatie word aangehaald dat de nationale wetgeving – in Nederland de Uitvoeringswet AVG – in Nederland niet is gebaseerd op artikel 10 van de Nederlandse Grondwet, maar op artikel 16 VwEU en de AVG.
406. Het was de bedoeling dat ook richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (ofwel 'E-privacyrichtlijn') per 25 mei 2018 zou worden vervangen door een Verordening met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie,maar dit is vooralsnog niet het geval.

geïnterpreteerd en toegepast. De gezamenlijke Europese toezichthouders publiceren via de Artikel 29-werkgroep (WP29) richtlijnenom een aantal begrippen uit de AVG en de toepassing daarvan te verduidelijken.[407] In vergelijking met de richtlijn legt de scope van de AVG de nadruk op: meer controle voor de betrokken personen over de gegevens die van hen verwerkt worden; meer verplichtingen voor de verwerkingsverantwoordelijke, inclusief een aantoon-plicht; effectiever toezicht en handhaving met verdergaande sancties en ten slotte een duidelijkere en bredere territoriale scope.[408]
Richtlijn 95/46/EG is vervangen vanwege een gewenste combinatie van continuïteit en innovatie[409]. De rechtstreekse werking van de verordening levert meer consistentie op. De AVG is een verordening, die een algemene strekking heeft, verbindend is in al haar onderdelen en rechtstreeks toepasselijk in elke Europese lidstaat.[410] Er is in de verordening ook ruimte voor flexibiliteit via de nationale uitvoeringswetten, zoals de Uitvoeringswet AVG in Nederland die in hoofdstuk 6 aan de orde komt.

Een belangrijke innovatie door de AVG is het geven van meer verantwoordelijkheden en verplichtingen aan de verwerkingsverantwoordelijke, waaronder de aantoonplicht. [411] Innovatie wordt ook verwacht op het terrein van effectievere toezicht en handhaving, onder andere via zogenoemde '*one-stop-shops*' voor burgers en bedrijven. *One-stop-shop* houdt in dat de bedrijven voortaan met slechts één leidende toezichthouder zaken hoeven te doen: de *lead supervisory authority*. Een laatste belangrijke reden voor aanpassing van de eerdere richtlijn is de territoriale scope van deze verordening. Het territoriale toepassingsgebied van de verordening is de verwerking van persoonsgegevens in het kader van de vestigingsverantwoordelijke of een verwerker in de Europese Unie, ongeacht of de verwerking in de Europese Unie al dan niet plaatsvindt. De scope van AVG omvat daarmee ook bedrijven die op de Europese markt opereren vanuit een vestiging elders in de wereld. Voor de markt van persoonlijke gezondheidsomgevingen, bijvoorbeeld via apps op smartphones, kan dit ook van groot belang zijn, omdat veel van de aanbiedende bedrijven zich buiten de EU bevinden.

In het vervolg van deze subparagraaf komen de hoofdlijnen van de AVG aan bod voor zover van belang voor dit onderzoek. Dit gebeurt via een toelichting van de structuur van de AVG aan de hand van relevante voorbeelden en bepalingen.[412]

De AVG bestaat uit een uitgebreidere structuur van regels dan richtlijn 95/46/EG. De structuur van AVG begint met een hoofdstuk algemene bepalingen met het onderwerp, de doelstellingen en het ruimere (territoriale) toepassingsgebied.

407. Zie Nouwt 2018. De door Nouwt genoemde richtlijnen van WP29 zijn te vinden via: ec.europa.eu/newsroom/article29/news.cfm?item_type=1358.
408. Zie Hustinx 2017, p.151-155.
409. Zie Hustinx, 2017, p.172.
410. Artikel 288 VwEU.
411. Idem.
412. Zie ook Van Balen & Nijveld (2017).

Ook de definities horen bij de algemene bepalingen en zijn ruimer dan bij de richtlijn (en in Nederland de Wbp). Aan het begrip persoonsgegeven zijn extra voorbeelden toegevoegd. Zoals gegevens over de verblijfplaats, een unieke identificatiecode, genderidentiteit en pseudonimisering[413]. Bovendien is de definitie meer afgebakend.[414] De definities van de verwerkingsverantwoordelijke en verwerker zijn in de AVG ook breder omschreven dan in de richtlijn.[415] Bovendien is de definitie van toestemming[416] in de AVG breder en verstrekkender geworden. Het begrip 'toestemming' is namelijk gedefinieerd als '*elke vrije, specifieke, op informatie berustende en uitdrukkelijke wilsuiting waarmee de betrokkene, door middel van hetzij een verklaring hetzij een ondubbelzinnige actieve handeling aanvaardt dat hem betreffende persoonsgegevens worden verwerkt*'. De verwerkingsverantwoordelijke en/of verwerker dienen/dient toestemming te krijgen uit een '*ondubbelzinnige actieve handeling*' van de betrokkene. De handeling moet een indicatie zijn van een wil waarmee de betrokkene een overeenstemming aantoont. De betrokkene (persoon) moet meteen inzicht hebben in wanneer het verwerken van persoonsgegevens gaat plaatsvinden. Daarnaast heeft de betrokkene de keuze om het verwerken van de persoonsgegevens te staken.

Na de algemene bepalingen volgt een tweede hoofdstuk met beginselen, zoals het rechtmatigheids-, doelbindings- en het nieuwe *accountability*-beginsel, oftewel de aantoonplicht. In tal van de artikelen worden mechanismen en procedures genoemd op grond waarvan een organisatie moet aantonen dat het technische of organisatorische maatregelen heeft genomen om de persoonsgegevens te beschermen. Het gaat om de volgende beginselen in artikel 5 AVG:

1. Rechtmatigheids-, behoorlijkheids- en transparantiebeginsel[417] (lid 1, onderdeel a);
2. Doelbindings- en verenigbaarheidsbeginsel (lid 1, onderdeel b);
3. Gegevensminimalisatie-beginsel (lid 1, onderdeel c);
4. Juistheidsbeginsel (lid 1, onderdeel d);
5. Opslagbeperkingsbeginsel (lid 1, onderdeel e)
6. Integriteits- en vertrouwelijksbeginsel (lid 1, onderdeel f)

413. Zie ook: Working Party 29, Richtlijnen over anonimiseren en pseudonimiseren, Advies 5/2014, (WP 216), goedgekeurd op 10 april 2014.
414. Persoonsgegeven, 'Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon' (artikel 4. lid 1 AVG).
415. De definitie van verwerker kwam al aan de orde. De definitie van verwerkingsverantwoordelijke is: 'Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen' (artikel 4 lid 7 AVG).
416. Zie ook, Working Party 29, Richtlijnen over toestemming (WP 259), op 28 november 2017 vastgesteld.
417. Zie Working Party 29, richtlijnen voor transparantie (WP 260), december 2017 gepubliceerd voor publieke consultatie.

7. Accountability-beginsel (lid 2).

Na de beginselen volgt een derde hoofdstuk met rechten van betrokkenen. Een belangrijk uitgangspunt in de AVG is dat iedereen in principe de mogelijkheid moet hebben om na te kunnen gaan waar gegevens over hem zijn vastgelegd en worden verwerkt.[418] Wie vindt dat gegevens onrechtmatig worden verwerkt kan dit civielrechtelijk dan wel bestuursrechtelijk aanvechten. Maar om dat te kunnen doen, moeten personen weten dat een organisatie persoonsgegevens over hen verwerkt.

In het vierde hoofdstuk van de AVG worden de verplichtingen voor de verwerkingsverantwoordelijke en de verwerker uitgewerkt. Die verplichtingen zijn verbreed. De belangrijkste voorwaarden voor verwerkingsverantwoordelijken en verwerkers zijn hierna kort op een rij gezet, vooral de voorwaarden met betrekking tot de zelfbeschikking over het verzamelen en vastleggen van gezondheidsgegevens.

1. Verbod op verwerken van bijzondere persoonsgegevens
Als hoofdregel verbiedt de AVG het verwerken van bijzondere persoonsgegevens.[419] Tot de categorie bijzondere persoonsgegevens behoren ook gezondheidsgegevens, inclusief genetische gegevens. Daarnaast is het als hoofdregel ook verboden om persoonsgegevens te verwerken over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, seksuele leven en lidmaatschap van een vakvereniging. De AVG voegt aan de bijzondere gegevens specifiek nog de categorie van biometrische gegevens toe. Biometrische gegevens zijn in de AVG als categorie van bijzondere persoonsgegevens opgenomen voor zover zij verwerkt worden met het oog op unieke identificatie van een persoon. Biometrische gegevens zijn onder meer vingerafdrukken, stem, handschrift, geometrie van de handomtrek en scans van netvlies, iris en gelaat. De gevoeligheid van deze exacte meetgegevens vloeit voort uit het feit dat ze unieke lichaamskenmerken van een persoon bevatten.

2. Ontheffingen op het verbod voor gezondheidsgegevens
Op dit algemene verbod op het verwerken van bijzondere persoonsgegevens bevat de AVG een aantal ontheffingen. De ontheffingen op het verbod om gezondheidsgegevens te verwerken, staan in artikel 9 lid 2 van de AVG. De Nederlandse uitwerking in de Uitvoeringswet AVG volgt in paragraaf 6.2.2.

3. Toestemming voor het verwerken van bijzondere persoonsgegevens
Als voor het verwerken van gezondheidsgegevens geen beroep kan worden gedaan op de hiervoor genoemde ontheffingen in de AVG en Uitvoeringswet

418. Met 'verwerken van persoonsgegevens' wordt overeenkomstig artikel 4 lid 2 AVG bedoeld: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
419. Artikel 8 en 10 AVG en artikel 22 t/m 31 Uitvoeringswet AVG.

AVG, dan kan het toch geoorloofd zijn om gezondheidsgegevens te verwerken, namelijk als de persoon daar uitdrukkelijke toestemming voor geeft.[420]

Met uitdrukkelijke toestemming is het toegestaan om bijzondere persoonsgegevens, zoals over iemands gezondheid, te verwerken. Anders dan voor 'ondubbelzinnige toestemming' geldt voor uitdrukkelijke toestemming dat de betrokkene daarover expliciet zijn wil moet hebben geuit. Een stilzwijgende of impliciete toestemming is niet uitdrukkelijk. De betrokkene moet in woord, schrift of gedrag uitdrukking hebben gegeven aan zijn wil om toestemming te verlenen voor de gegevensverwerking. Op de verwerkingsverantwoordelijke rust een dubbele bewijslast om aan te mogen nemen dat iemand uitdrukkelijk toestemming heeft gegeven. Zo moet bij twijfel bewezen kunnen worden dat een bepaalde toestemming is verleend en waarvoor. Bovendien zal zo nodig aangetoond moeten kunnen worden dat de toestemming aan de gestelde eisen voldoet. De verantwoordelijke zal dan ook moeten kunnen aantonen dat hij bijvoorbeeld wat betreft informatieverstrekking aan betrokkene alles heeft gedaan wat redelijkerwijs van hem mocht worden verwacht. De toestemming is niet geldig als zij niet voldoet aan deze vereisten.

4. Grondslag gegevensverwerking
Wie persoonsgegevens in het algemeen verwerkt moet dat kunnen baseren op ten minste een van de grondslagen in artikel 6 AVG. Dat geldt ook voor gezondheidsgegevens.

Een mogelijke grondslag kan zijn dat het verzamelen, vastleggen en verder gebruiken van persoonsgegevens over iemands gezondheid noodzakelijk is ter uitvoering van een overeenkomst tot geneeskundige behandeling[421] of dat dit voortvloeit uit de wettelijke dossierplicht[422].
Ook de 'ondubbelzinnige toestemming' van de betrokkene[423] is een mogelijke grondslag voor het verzamelen en vastleggen van persoonsgegevens. Wanneer een beroep op andere grondslagen kan worden gedaan, is de toestemming van de betrokkene echter niet nodig.

5. Overige bepalingen voor verwerkingsverantwoordelijken en verwerkers
De AVG kent uiteraard nog meer bepalingen die van toepassing zijn op het verwerken van gezondheidsgegevens. In aansluiting op andere wetten is bepaald dat persoonsgegevens uitsluitend op een behoorlijke en zorgvuldige wijze mogen worden verwerkt.[424] Hiermee wordt aangesloten bij de zorgvuldigheidsnormen uit het burgerlijk recht, zoals de onrechtmatige daad. Bij het bestuursrecht gaat het in het bijzonder om de algemene beginselen van behoorlijk bestuur.

Wanneer persoonsgegevens eenmaal zijn verzameld zal de verwerkingsverantwoordelijke die gegevens ook verder willen verwerken. De hoofdregel is dat

420. Artikel 9 lid 2 AVG.
421. Artikel 6 lid 1 sub b AVG.
422. Artikel 7:454 BW, oftewel een wettelijke grondslag in de zin van artikel 6 sub c AVG.
423. Artikel 6 sub a AVG.
424. Artikel 5 lid 1, onderdeel a AVG.

verder verwerken van persoonsgegevens alleen is toegestaan op een wijze die 'niet onverenigbaar' is met de doeleinden waarvoor ze zijn verkregen.[425]
De AVG kent geen specifieke bewaartermijn voor persoonsgegevens. De algemene regel is dat persoonsgegevens in een tot personen herleidbare vorm niet langer bewaard mogen worden dan noodzakelijk is voor het doel waarvoor ze zijn verzameld of vervolgens worden verwerkt.[426]
Tot slot is er de algemene verplichting die op een verwerkingsverantwoordelijke rust om passende technische en organisatorische maatregelen te treffen teneinde persoonsgegevens te kunnen beveiligen tegen verlies of enige andere vorm van onrechtmatige verwerking, zoals onrechtmatige toegang tot gezondheidsgegevens.[427] Deze verplichting omvat ook het dataminimalisatiebeginsel dat niet meer gegevens verwerkt mogen worden dan noodzakelijk. Daarmee is deze verplichting tevens een stimulans voor *data protection-by-design*, dat in hoofdstuk 7 verder wordt uitgewerkt.

Informatierechten
Binnen de AVG worden informatierechten als hoeksteen beschouwd. De veronderstelling daarbij is dat een persoon ook daadwerkelijk zijn recht kan uitoefenen, omdat hij weet dat er informatie over hem wordt verwerkt en door wie. Mede vanuit de gedachte dat dit bijdraagt aan de informationele zelfbeschikking van een persoon en hem meer controle biedt over gegevensverwerking. Dit uitgangspunt is ook te vinden in de in het volgende hoofdstuk over Nederland te bespreken 'Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg' die 1 juli 2017 in werking is getreden met een overgangstermijn van drie jaren voor de nieuwe, actieve zelfbeschikkingsrechten 'elektronische inzage' en 'gespecificeerde toestemming'.

Daarnaast krijgen personen en verwerkingsverantwoordelijken van bijvoorbeeld persoonlijke gezondheidsomgevingen door de AVG onder andere de volgende aanvullende rechten en verplichtingen: de genoemde verantwoordingsplicht (*accountability*, artikel 5, lid 2), het recht op vergetelheid/gegevenswissing (artikel 17), dataportabiliteit (artikel 20), *data protection by design* (artikel 25) en gegevensbeschermingseffectbeoordeling (artikel 35).

Voor persoonlijke gezondheidsomgevingen is in vergelijking met de richtlijn onder andere het nieuwe recht op dataportabiliteit van belang. Dit nieuwe recht is nauw verbonden met het recht op inzage, maar verschilt hier ook van. Het recht op dataportabiliteit betreft de overdraagbaarheid van gegevens. Het houdt in dat de persoon het recht heeft de persoonsgegevens die hij aan een verantwoordelijke heeft verstrekt in een gestructureerde, gangbare en machineleesbare vorm te ontvangen, zodat hij deze aan een andere verantwoordelijke kan overdragen. Het doel van dit nieuwe recht is de positie van personen te versterken en hun meer controle over hun gegevens te geven. Voor persoonlijke gezondheidsomgevingen is het recht op dataportabiliteit van toepassing voor

425. Artikel 5 lid 1, onderdeel b, artikel 6 lid 4 en artikel 89 AVG.
426. Artikel 5 lid 1, onderdeel e en artikel 89 AVG.
427. Artikel 32 AVG.

zover gegevens in een medisch dossier of persoonlijke gezondheidsomgeving door de betrokkene zelf zijn verstrekt aan de zorgaanbieder of de leverancier van een persoonlijke gezondheidsomgeving. Dit nieuwe recht is een stimulans voor het tot stand komen van persoonlijke gezondheidsomgevingen, omdat het succes hiervan staat of valt met de mogelijkheid om gegevens over te dragen. Bij een recht op dataportabiliteit voor alle gegevens in een medisch dossier of persoonlijke gezondheidsomgeving van de betrokkene zou de ontwikkeling van persoonlijke gezondheidsomgevingen nog meer bijdragen aan informationele zelfbeschikking. Aan de andere kan het recht op dataportabiliteit er ook toe leiden dat andere (ook kwaadwillende) partijen eenvoudiger de beschikking kunnen krijgen over de gezondheidsgegevens in de persoonlijke gezondheidsomgevingen. Aanvullende juridische, organisatorische en technologische maatregelen om gezondheidsgegevens – met name buiten de zorgcontext – te beschermen zijn door het recht op dataportabiliteit daarmee extra van belang. In die zin biedt de AVG ook zelf al waarborgen tegen kwaadwillenden, maar houdt de AVG niet specifiek rekening met persoonlijke gezondheidsomgevingen. Dat past bij het uitgangspunt dat de AVG technologieneutraal dient te zijn.

In het vijfde hoofdstuk van de AVG komt de doorgifte van persoonsgegevens aan derde landen of internationale organisaties aan bod. Dit is voor de praktijk van persoonlijke gezondheidsomgevingen een belangrijk hoofdstuk, omdat op dit moment en in de nabije toekomst veel verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen gevestigd zijn buiten de Europese Unie. Bij de territoriale toepassing van de AVG kwam al even aan de orde dat het territoriale toepassingsgebied van de verordening de verwerking van persoonsgegevens in het kader van de vestigingsverantwoordelijke of een verwerker in de Europese Unie is, ongeacht of de verwerking in de Europese Unie al dan niet plaatsvindt.

Het zesde hoofdstuk van de AVG gaat over onafhankelijke toezichthoudende autoriteiten.
Het toezicht door de Autoriteit persoonsgegevens (AP) en andere toezichthouders komt hierna in hoofdstuk 7 over rechtsbescherming aan de orde. Hier wordt ter illustratie benoemd dat artikel 58 AVG de AP 26 bevoegdheden geeft, waaronder een grotere boetebevoegdheid. Met de komst van de AVG gaan de maximale boetes voor schending van regels uit de AVG omhoog naar € 10 miljoen of (als dat laatste meer is) 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar. Voor bepaalde schendingen of het niet opvolgen van bevelen kunnen de boetes zelfs oplopen tot het dubbele daarvan.

Het zevende hoofdstuk van de AVG gaat over samenwerking tussen de leidende toezichthoudende autoriteiten en de andere toezichthoudende autoriteiten. Bij persoonlijke gezondheidsomgevingen zijn ook internationale multinationals betrokken. Bij het toezicht hierop is geregeld hoe toezichthouders binnen Europa elkaar wederzijdse bijstand kunnen verlenen. De '*one-stop-shop*' kwam hiervoor al aan de orde.

Het achtste hoofdstuk gaat over beroep, aansprakelijkheid en sancties. Het negende hoofdstuk van de AVG gaat over specifieke situaties. Het tiende hoofdstuk bevat gedelegeerde en uitvoeringsbepalingen en het laatste hoofdstuk bevat slotbepalingen.

5.4 RECHTSPRAAK EHRM

Wat betreft de jurisprudentie van het EHRM en de Europese Commissie voor de Rechten van de Mens (ECRM), ten aanzien van informationele zelfbeschikking, is er voornamelijk jurisprudentie met betrekking tot artikel 8 EVRM.[428] In de praktijk draait het in de uitspraken van het Hof op basis van artikel 8 EVRM steeds om de vraag of het beoogde doel te realiseren is en zo ja, of de desbetreffende beperking dan in een redelijke verhouding staat tot dat beoogde doel en of er geen minder vergaande beperkingen denkbaar zijn om hetzelfde doel te bereiken.

Op grond van artikel 8, lid 1 EVRM, heeft iedereen het recht op respect voor zijn privé-, familie- en gezinsleven, zijn woning en zijn correspondentie. Krachtens lid 2 zijn inbreuken op deze vrijheden door overheidsautoriteiten slechts toegestaan indien ze in overeenstemming zijn met de wet, en noodzakelijk zijn in een democratische samenleving. Het EHRM heeft onder andere in de zaak Silver e.a. t. Verenigd Koninkrijk de criteria voor toetsing aan artikel 8, lid 2, EVRM verder uitgewerkt.[429] Wat betreft de eis van overeenstemming met de wet, hanteert het EHRM een ruim wetsbegrip waardoor lagere regelgeving en ongeschreven recht hier ook onder vallen, zolang ze voor de burger toegankelijk en voorzienbaar zijn op grond van nauwkeurige formulering. De ernst van de inbreuk op een recht is van belang voor de eisen die aan de wet worden gesteld.[430] Hierboven zijn de doelcriteria uit lid 2 benoemd die een inbreuk op lid 1 kunnen rechtvaardigen. De nadruk ligt echter vooral op de noodzakelijkheid om deze doelen te bereiken. De beperking moet noodzakelijk zijn in een democratische samenleving. Hiertoe moet er sprake zijn van een dringende maatschappelijke behoefte. De beperking moet evenredig zijn aan het nagestreefde doel. Tevens moeten er relevante en toereikende gronden voor beperking van het recht zijn. Hier moet het Hof dus belangen afwegen, waarbij de Staat ook een beoordelingsvrijheid heeft, die vervolgens ook per geval wordt getoetst door het Hof.
In dit krachtenveld moet het EHRM opereren wanneer ze een uitspraak doet of een verdragsstaat al dan niet in strijd heeft gehandeld met het verdrag. Dit geldt ook voor artikel 8 EVRM en het recht op privacy. Hieronder worden de belangrijkste arresten van het Hof besproken met betrekking tot de informatiepositie aangaande persoonlijke gegevens. In deze zaken gaat het Hof niet expliciet uit van een recht op informationele zelfbeschikking, maar refereert het Hof hier wel impliciet aan als een facet van het recht op privacy.[431]

428. Zie ook Van Dijk 2006.
429. ECRM 25 maart 1983, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75 (Silver e.a. t. Verenigd Koninkrijk).
430. EHRM 2 augustus 1984, nr. 8691/79 (*Malone*).
431. De Hert & Gutwirth 2009, p. 19; De Hert 1998, p. 7.

5.4.1 Informationele zelfbeschikking in de zaak Malone

Expliciet komt het begrip informationele zelfbeschikking aan de orde in de zaak Malone, waarbij de verzoeker klaagt over schending van artikel 8 vanwege onderschepping van de post, het afluisteren van de telefoon en het registreren van gebelde nummers door de Britse politie.[432] Het Hof acht dit een inbreuk op artikel 8 EVRM die niet gerechtvaardigd kan worden, aangezien een grondslag in het Britse recht ontbreekt voor deze acties van de politie. Rechter Petitti is het met deze conclusie eens, maar vindt dat het Hof het Britse systeem wel uitgebreider onder de loep had kunnen nemen. Petitti schetst een grote bedreiging voor democratische samenlevingen vanaf de jaren tachtig vanwege de neiging van overheidsautoriteiten om het complete leven van burgers te registreren. Hij geeft diverse voorbeelden van inbreuken in het privéleven van burgers. Vanwege de vele misstanden is er wel degelijk wetgeving gekomen om dit in te perken. Maar toch zitten hier vaak lacunes volgens Petitti. Dit heeft onder andere te maken met het feit dat de uitvoerende macht graag zelf de touwtjes in handen houdt, zonder controle van de rechterlijke macht. Ook onderhavige zaak is volgens Petitti weer een voorbeeld dat de wettelijke bescherming van privacy niet goed geregeld is. Hij wil dat graag verder uitwerken, door verder te gaan dan de conclusie van het Hof dat een wettelijke basis voor de inbreuk ontbreekt.

Petitti geeft aan dat het belangrijk is onderscheid te maken in de wet tussen verschillende situaties waarin inbreuk wordt gemaakt op het privéleven, bijvoorbeeld door het onderscheppen van telefonische communicatie. Daarnaast moet onderscheid gemaakt worden tussen machtiging van de rechter om een inbreuk te maken op de privacy, en machtiging van een minister. Petitti vindt ook dat het recht op toegang tot gegevensbanken moet worden gewaarborgd, door de persoon in staat te stellen op de hoogte te zijn van gegevensbanken waar zijn gegevens worden opgeslagen en deze gegevens te kunnen betwisten, met uitzondering van het geval van justitieel onderzoek naar deze persoon. Vervolgens geeft hij aan dat de aard en implicaties van gegevensverwerking totaal veranderd zijn met de digitalisering. Petitti vindt het dan ook terecht dat het Duitse Constitutioneel Hof het concept van informationele zelfbeschikking heeft ontwikkeld, waarbij een persoon het recht heeft zelf te beslissen over de openbaarmaking van de gegevens in verband met zijn privéleven en om zichzelf te beschermen tegen een toenemende tendens om hem publiek bezit te maken. Hij vindt dat er ook op Europees niveau steviger standaarden moeten worden vastgesteld om inbreuken op artikel 8 EVRM aan af te meten. Met betrekking tot gegevensbanken ziet hij hier ook ontwikkelingen. De marge van beoordeling van lidstaten is van belang, maar Petitti acht de bescherming van de privacy zo belangrijk dat hier op Europees niveau een dikkere streep in het zand moet worden getrokken. Hij concludeert: ‘de Conventie beschermt de menselijke gemeenschap; de mens heeft in onze tijd de behoefte om zijn identiteit te beschermen, om totale transparantie van de maatschappij te weigeren, en om zijn persoonlijke privacy te behouden.’ Petitti bevestigt met andere woorden het belang van informationele zelfbeschikking voor de menselijke waardigheid.

432. EHRM 2 augustus 1984, nr. 8691/79 (Malone).

5.4.2 EHRM over privacy

Hierna volgt een aantal uitspraken van het EHRM over privacy in het licht van informationele zelfbeschikking. Verderop volgt een aantal uitspraken van het EHRM met betrekking tot de bescherming van persoonsgegevens en in het bijzonder de bescherming van gezondheidsgegevens.

5.4.3 DNA-testen

Impliciet ging een aantal zaken van het EHRM over informationele zelfbeschikking waarin kinderen achter de identiteit van hun ouders proberen te komen. Actief toegang hebben tot informatie over de eigen ouders is volgens deze rechtspraak namelijk een fundamenteel onderdeel van het kunnen inrichten van iemands persoonlijke leven en de vorming van een eigen identiteit.

In de zaak Mikulic[433] klaagt een meisje tegen de staat Kroatië over het gebrek aan juridische mogelijkheden om de man die beweert haar vader te zijn, te dwingen om mee te werken aan een vaderschapstest. Het belang van het meisje om een belangrijk aspect van haar persoonlijke identiteit te weten te komen, en daarmee zelf te beschikken over openbaarmaking van persoonlijke gegevens, is door het Hof afgewogen tegen het belang om zelf te kunnen bepalen mee te willen werken aan een medische test. Dit kan ook onder informationele zelfbeschikking worden geschaard. Het Hof oordeelt dat er een onevenredige inbreuk is gemaakt op de belangen van de klager. Het meisje zit namelijk zo lang in onzekerheid over haar persoonlijke identiteit dat Kroatië hiertegen maatregelen moet treffen. De informationele zelfbeschikking van het meisje is hier door het Hof dus boven de informationele zelfbeschikking van de vader geplaatst. Impliciet, want het Hof gaat niet expliciet uit van een recht op informationele zelfbeschikking.

De Odièvre-zaak[434] gaat eveneens over een kind dat achter de identiteit van een ouder wilde komen. In dit geval wil het geadopteerde kind te weten komen wie haar natuurlijke moeder is. De moeder heeft het kind achtergelaten bij haar geboorte met het uitdrukkelijke verzoek om nooit haar identiteit te onthullen. Het Hof oordeelt dat deze kwestie van een andere orde is dan die over vaderschapstesten. Opnieuw ziet het Hof een strijd tussen twee belangen. Het belang van het kind om te weten te komen waar het vandaan komt, en het belang van de moeder om een kind veilig ter wereld te brengen en anoniem te blijven. Hier zijn dus opnieuw twee kanten van informationele zelfbeschikking impliciet zichtbaar. Het Hof komt niet tot een schending van artikel 8 EVRM door Frankrijk. In Frankrijk is er een wet die het mogelijk maakt voor moeders om anoniem een kind op de wereld te zetten, maar tegelijkertijd is er een wet die het mogelijk maakt voor kinderen om te zoeken naar hun afkomst. Zo wordt er in de Franse wetgeving geprobeerd een balans te vinden tussen de belangen van moeders en die van kinderen. In het geval van Odièvre

433. EHRM 7 februari 2002 (*Mikulic t. Kroatië*).
434. EHRM 13 februari 2003 (*Odièvre t. Frankrijk*).

prevaleert het belang van de moeder. Haar identiteit kan volgens de Franse wetgeving geheim blijven. Het Hof acht de wijze waarop Frankrijk dit heeft vormgegeven te rechtvaardigen.

De mogelijkheden voor toepassing van DNA-testen zijn steeds verder gevorderd. Het EHRM is daarom op een gegeven moment geconfronteerd met de vraag of een DNA-analyse op een dood persoon geoorloofd is. Bijvoorbeeld in de zaak Jäggi[435], waar het gaat om een DNA-analyse op een dood persoon. In deze zaak erkent het Hof het recht op een identiteit, waaronder begrepen het recht om te weten wie je ouders zijn, als een belangrijk onderdeel van privéleven. Dit is volgens het Hof voldoende reden om een DNA-analyse uit te voeren op een dood persoon. Evenals in de zaak Ervan van KFM t. Denemarken[436] bepaalt het Hof dat DNA-tests op een dode geen inbreuk vormen op het privéleven van de dode persoon. Er is daarmee geen beletsel om DNA-tests op een dood persoon uit te voeren om daarmee de identiteit van ouders te achterhalen.

Uit de zaak Ebru & Tayfun Engin Colak[437] blijkt dat het EHRM soms ook beslist tot bescherming van vermeende ouders, door ervoor te zorgen dat ze niet gedwongen kunnen worden tot DNA-tests. In deze zaak wordt bepaald dat een systeem waarin een vermeende vader niet gedwongen kan worden tot het meewerken aan een gerechtelijk bevel voor het ondergaan van een DNA-test, in principe verenigbaar is met het EVRM. Dat kan echter alleen in overeenstemming met het proportionaliteitsprincipe, indien er alternatieven zijn om een onafhankelijke autoriteit snel tot een beslissing te laten komen over de vaderschapsclaim, en als er consequenties zijn verbonden aan de weigering om mee te werken aan een DNA-test.

5.4.4 Toegang dossiers sociale dienst

M.G. t. Verenigd Koninkrijk[438] betreft een zaak waarin wordt geklaagd over een gebrek aan onbelemmerde toegang tot gegevens van de sociale dienst. De klager wilde toegang tot deze dossiers om informatie over zijn jeugd naar boven te krijgen, waardoor hij kan achterhalen of hij was misbruikt door zijn vader. Deze informatie zou hem helpen om zijn psychische problemen te verklaren. Hij kreeg geen toegang tot de dossiers en had ook geen mogelijkheid om tegen deze weigering in beroep te gaan bij de autoriteiten. Het Hof concludeerde daarom dat het Verenigd Koninkrijk niet voldeed aan de verplichting om het privéleven van de klager te beschermen. Het recht op toegang, en daarmee ook het recht om zelf te beschikken over het gebruik van persoonlijke gegevens, is in deze zaak in het geding, en wordt volgens het Hof niet afdoende beschermd door het Verenigd Koninkrijk. Met andere woorden kon de klager volgens het EHRM aanspraak maken op informationele zelfbeschikking, zij het impliciet.

435. EHRM 13 juli 2006 (*Jäggi t. Zwitserland*).
436. EHRM 15 mei 2006 (*Erven Kresten Filtenborg Mortensen t. Denemarken*).
437. EHRM 30 mei 2006 (*Ebru & Tayfun Engin Colak*).
438. EHRM 24 september 2002 (*M.G. t. Verenigd Koninkrijk*).

5.4.5 Publicatie foto's

In de zaak Nikolaishvili[439] bepaalt het EHRM dat het begrip privéleven elementen omvat die betrekking hebben op de persoonlijke identiteit, zoals de naam of een beeld. De publicatie van een foto van iemand valt onder artikel 8 EVRM, ook in het geval dit een publiek figuur is. Het Hof maakt wel een onderscheid tussen gewone en publieke personen. Uit Sciacca t. Italië[440] wordt duidelijk dat als het gaat om gewone personen de interpretatie van privéleven ruimer is, ook als het gaat om zaken die zich in het publieke leven afspelen. Bij een publiek figuur is meer geoorloofd, ook in de zin van kritiek, dan bij een gewoon persoon zo blijkt bijvoorbeeld uit Von Hannover[441]. Toch bepaalt het Hof in deze zaak dat ook publieke figuren recht hebben op een legitieme verwachting ten aanzien van bescherming en respect voor het privéleven. Daarbij is volgens het Hof meer waakzaamheid geboden, vanwege nieuwe communicatietechnologieën, die het mogelijk maken om persoonlijke gegevens op te slaan en te reproduceren.

Als het gaat om het vinden van de balans tussen informationele zelfbeschikking en de vrijheid van meningsuiting dan kijkt het Hof ook of de foto's, of artikelen, een bijdrage leveren aan het debat in het algemeen belang van de maatschappij. In het geval van Biriuk[442] gaat het om publicatie van een artikel over de medische toestand van de klager met betrekking tot haar seksuele leven. Het Hof heeft geoordeeld dat dit niet leidde tot een bijdrage aan het debat in het algemeen belang van de maatschappij, maar slechts gericht was op de zucht naar sensatie van bepaalde groepen lezers.

5.4.6 Het recht op naamswijziging

In Daroczy t. Hongarije[443] laat het Hof zich uit over het recht op naamswijziging. De naam is ook direct verbonden aan de persoonlijke identiteit, en daarmee aan het privéleven. Als het gaat om het recht op naamswijziging dan is dat dus ook verbonden met het recht op privéleven. Het Hof vindt dat hier in het algemeen belang regels aan mogen worden gesteld. Dat blijkt ook uit de Finse zaak Stjerna[444]. Meneer Stjerna wilde zijn Zweedse naam laten wijzigen in de naam van één van zijn voorouders. Het Hof achtte de weigering van Finland niet ongerechtvaardigd vanwege het daarmee gediende publieke belang. Het ongemak voor de klager werd tevens niet groot genoeg gevonden. Ook in Burghartz t. Zwitserland[445] geeft het Hof aan dat de naam van een individu is gekoppeld aan het recht op privéleven. Het hebben van een eigen naam en de vraag of men deze kan wijzigen is dus een vraag die dient te worden afgewogen in het kader van informationele zelfbeschikking.

439. EHRM 13 januari 2009, 37048/04 [2009] ECHR 63 (*Giorgi Nikolaishvili t. Georgië*).
440. EHRM 11 januari 2005 (*Sciacca t. Italië*).
441. EHRM 24 juni 2004 (*Caroline von Hannover t. Duitsland*).
442. EHRM 25 november 2008 (*Biriuk t. Litouwen*).
443. EHRM 1 juli 2008 (*Daroczy t. Hongarije).*
444. EHRM 25 november 1994 (*Stjerna t. Finland*).
445. EHRM 22 februari 1994 (*Burghartz t. Zwitserland*).

5.4.7 Verloren ID-kaart niet terug gegeven

In Smirnova t. Rusland[446] draait het om een identiteitskaart die niet is teruggegeven. Bij de arrestatie is deze ingenomen en nooit teruggegeven. Daardoor kan ze niet aan werk komen, niet trouwen en krijgt ze een administratieve boete wegens de onmogelijkheid om zich te kunnen identificeren. Het Hof oordeelt dat artikel 8 EVRM is geschonden en legt een directe link tussen de plicht om je als burger te identificeren en het recht op een privéleven.

5.4.8 Identiteit en het algemeen persoonlijkheidsrecht

Impliciet ging het in de behandelde zaken van het EHRM over informationele zelfbeschikking waarbij personen achter hun identiteit probeerden te komen. Volgens het EHRM is het behoud van een geestelijk stabiele toestand een onmisbare voorwaarde voor het recht op privéleven. Dat betekent dat iedereen groot belang heeft bij informatie over de eigen identiteit, waaronder informatie op basis waarvan de identiteit van de ouders kan worden begrepen en informatie over de kindertijd en vroege ontwikkeling. Dat werd duidelijk uit de zaken die hiervoor werden besproken. Om achter de identiteit van een persoon te komen is ook het gebruik van technologieën, als DNA-tests, aan de orde, vandaar dat het Hof zich hierover heeft uitgesproken.
Concluderend kan worden gesteld dat in de jurisprudentie van het EHRM een ontwikkeling van een recht op identiteit te zien is, wegens de bescherming van achternaam, voornaam, geslacht en toegang tot gegevens over de eigen afkomst. Dit kan worden gekoppeld aan het algemeen persoonlijkheidsrecht, dat zowel in Nederland als in Duitsland is erkend, wat vervolgens weer kan dienen als fundament voor informationele zelfbeschikking.

5.4.9 EHRM over bescherming van persoonsgegevens

In de jaren tachtig heeft het EHRM de bescherming van persoonsgegevens in grotere mate onder het bereik van artikel 8 EVRM gebracht. Daar komt het Verdrag van Straatsburg bij, dat als uitwerking van de positieve verplichting van de lidstaten ten aanzien van artikel 8 EVRM kan worden beschouwd.
De Hert en Gutwirth[447] zien het EHRM criteria bepalen voor het verwerken van persoonsgegevens. Het komt erop neer dat gegevensverwerking niet buitensporig, onnodig of ongerechtvaardigd mag zijn.[448] De Hert en Gutwirth constateren dat het Hof echter geen verdere criteria bepaalt voor wat dan buitensporige, onnodige of ongerechtvaardigde vormen van gegevensverwerking zijn.

Allereerst volgt een vergelijking van gegevensbeschermingsjurisprudentie op basis van het EVRM met enkele belangrijke principes uit het gegevensbeschermingsrecht.[449]

446. EHRM 24 juli 2003 (*Smirnova t. Rusland*).
447. De Hert & Gutwirth 2009.
448. Diezelfde criteria komen terug in artikel 6 (1) (c) en artikel 7 (c, e) van richtlijn 95/46/EG.
449. Daarbij is niet alleen artikel 8, maar zijn ook artikel 5, 6, 10, 11 en 13 EVRM van toepassing.

Het Hof erkent het doelbindingsbeginsel onder andere in de zaak Peck[450], wat inhoudt dat gegevens alleen voor specifieke doeleinden gebruikt mogen worden. Het Hof heeft in de zaak Amann[451] bepaald dat overheidsautoriteiten slechts gegevens mogen verzamelen wanneer dat relevant is en een concrete verdenking daaraan ten grondslag ligt.[452] Dit beginsel houdt in dat gegevens niet voor een ander doel mogen worden gebruikt dan omschreven, en de begrenzing van openbaarmaking van persoonsgegevens aan derden. Op deze beginselen is geen uitzondering mogelijk in het gegevensbeschermingsrecht, waar dat via artikel 8 lid 2 EVRM volgens het Hof wel mogelijk is. De Hert geeft aan dat de formulering van deze uitzonderingsbepalingen ook ruim is en dat de jurisprudentie tekortschiet als het gaat om het stellen van eisen aan doeleinden om artikel 8 EVRM te beperken.

Eveneens is de mogelijkheid tot inzage in het gegevensbeschermingsrecht[453] vastgelegd. Hierop wordt alleen een uitzondering gemaakt voor politie- en veiligheidsdiensten. Dit is ook het geval in de jurisprudentie van het EHRM. Zo zien we in de zaken Klass[454] en Leander[455] dat het in het kader van de strafrechtspleging geoorloofd is om personen niet te informeren over opslag van hun persoonsgegevens.
Daarnaast geeft het gegevensbeschermingsrecht een recht op inzage in en correctie van persoonsgegevens. Ook hier is een uitzondering gemaakt voor politie- en veiligheidsdiensten. De jurisprudentie van het EHRM inzake artikel 8 EVRM sluit hier opnieuw bij aan, zo zien we in de zaken Klass, Leander, Martin[456] en Gaskin[457]. Artikel 5, 6, 8, 10, 13 EVRM bieden wel degelijk bescherming als het gaat om inzage en correctie.

Op deze manier valt voor de verschillende principes van het gegevensbeschermingsrecht een vergelijking te maken met het EVRM ten aanzien van de bescherming van persoonsgegevens. Naast bovenstaande vergelijking is te zien dat de bescherming van persoonsgegevens door het EHRM ruimer is ten aanzien van het recht op een eerlijk proces[458] en het recht op privéleven, correspondentie en het familieleven.[459] De reikwijdte van het EVRM is volgens De Hert ook groter dan het gegevensbeschermingsrecht omdat het gegevensbeschermingsrecht zich beperkt tot verwerking van persoonsgegevens. Dat heeft ermee te maken dat het voor het EHRM niet uitmaakt wie de informatiehouder van de persoonsgegevens is, en op welke wijze de informatie wordt gebruikt, maar slechts of de aard van de informatie relevant is gegeven het beschermingsbereik van het EVRM.

450. EHRM 28 januari 2003 (*Peck t. VK*).
451. EHRM 16 februari 2000 (*Amann t. Zwitserland*).
452. In artikel 6b, 16, 17 richtlijn 95/46/EG en artikel 5b jo. 7 Verdrag van Straatsburg is het doelbindingsbeginsel vastgelegd.
453. Artikel 8 Verdrag van Straatsburg; art. 10 en 11 richtlijn 95/46/EG.
454. EHRM 6 september 1978 (*Klass e.a. t. Duitsland*).
455. EHRM 26 maart 1987 (*Leander t. Zweden*).
456. EHRM 30 mei 2013, nr. 35985/09 (*Martin t. Estland*).
457. EHRM 7 juli 1989 (*Gaskin t. VK*).
458. Artikel 6 EVRM.
459. Artikel 8 EVRM.

Anderzijds biedt het EVRM ook minder bescherming aan persoonsgegevens dan het gegevensbeschermingsrecht. Zo biedt artikel 8 EVRM geen bescherming ten aanzien van alle persoonsgegevens, maar slechts voor bepaalde categorieën. Aldus worden alleen die gegevens beschermd, die kunnen worden gerelateerd aan een recht of vrijheid. Deze beperking doet zich vooral gelden bij het recht op eerbiediging van het privéleven. De aard en mate van intimiteit van de gegevens bepalen volgens het Hof of ze privacygevoelig zijn en daarmee onder de bescherming van artikel 8 EVRM vallen. Persoonsgegevens die 'niet privé genoeg' zijn, worden daarmee niet beschermd. De zaak Reyntjens[460] is een duidelijk voorbeeld, aangezien de identiteitskaart van de heer Reyntjens, waarvan de gegevens door de autoriteiten werden geregistreerd, niet als privacygevoelig werd aangemerkt en daarmee niet in aanmerking kwam voor bescherming onder artikel 8 EVRM.
Daarnaast is te constateren dat het Hof op bepaalde onderdelen van bescherming van persoonsgegevens minder strenge eisen aanlegt. Het gegevensbeschermingsrecht heeft een toegevoegde waarde ten opzichte van het EVRM ten aanzien van de bescherming van persoonsgegevens. Niet alle principes uit het gegevensbeschermingsrecht worden namelijk door het EHRM toegepast. Hieronder komen enkele toonaangevende zaken uit de EHRM-jurisprudentie ten aanzien van privacy en bescherming van persoonsgegevens aan bod, in relatie tot het concept van informationele zelfbeschikking.

5.4.10 De zaak Leander

In 1987 doet het EHRM een belangrijke uitspraak ten aanzien van de bescherming van persoonsgegevens. De zaak Leander draait om belastende gegevens ten aanzien van de heer Leander in het register van de geheime politie. Leander kreeg zelf geen inzage in de informatie over hem, maar tegelijkertijd was deze informatie wel bekend voor potentiële werkgevers, wat een beletsel betekende om aan het werk te kunnen en tot zijn ontslag had geleid. Het Hof concludeerde op basis van artikel 8 EVRM dat het geheime politieregister informatie bevatte met betrekking tot het privéleven van Leander. Het register vormt een inbreuk op deze vrijheid, maar is volgens het Hof op grond van artikel 8, lid 2, EVRM gerechtvaardigd in het kader van de nationale veiligheid. Voorwaarde is dat door een dergelijk register kan worden voorkomen dat Leander in publieke dienst treedt. Het Hof laat de Staat een ruime beoordelingsvrijheid voor de dringende maatschappelijke behoefte om een dergelijke maatregel te treffen.
In de zaak Leander is het recht op toegang tot informatie in het geding. Leander heeft niet de mogelijkheid om zelf te beschikken over openbaarmaking en gebruik van zijn persoonlijke gegevens, maar dit acht de rechter gerechtvaardigd in het licht van de omstandigheden. Het gegevensbeschermingsrecht blijkt tamelijk machteloos ten opzichte van 'geheime' inlichtingendiensten.
De Hert en Gutwirth concluderen hier dat de bescherming van het EVRM tekortschiet vanuit het oogpunt van bescherming van persoonsgegevens. Artikel 8 EVRM geeft volgens het EHRM namelijk geen algemeen recht op toegang tot

460. EHRM 9 september 1992 (*Reyntjens t. België*).

persoonsgegevens.[461] Vervolgens wordt er ook onderscheid gemaakt tussen persoonsgegevens die direct het privéleven raken en persoonsgegevens waar dat niet het geval is. In het gegevensbeschermingsrecht is hiervan, behoudens de erkenning van speciale categorieën gevoelige gegevens, geen sprake.

5.4.11 EHRM over bescherming van gezondheidsgegevens

In het licht van deze dissertatie is in het bijzonder de rechtspraak van het EHRM over gezondheidsgegevens relevant.[462] Het EHRM heeft een uitgebreide jurisprudentie opgebouwd ten aanzien van de bescherming van gezondheidsgegevens. Uit de jurisprudentie blijkt dat de informatie in een medisch document betrekking heeft op het privéleven, aangezien het persoonlijke en gevoelige informatie betreft over de persoonlijke gezondheid. Het EHRM stelt in *Trocellier t. Frankrijk*[463] dat toegang tot eigen gezondheidsgegevens bij geneeskundige behandelingen noodzakelijk is.

Bescherming van gezondheidsgegevens op grond van artikel 8 EVRM komt aan de orde in de uitspraak van het EHRM in de zaak I. t. Finland.[464] Volgens het Europese Hof overtrad het Finse ziekenhuis artikel 8 EVRM. De vertrouwelijkheid van het medisch dossier valt hier namelijk ook onder. Onder de zorgplicht van het ziekenhuis, valt onder meer de plicht tot beveiliging van gezondheidsgegevens tegen kennisneming door ongeautoriseerde raadplegers en de plicht om het gebruik van elektronische patiëntendossiers te controleren door middel van de logbestanden.

In I. t. Finland draait het om de beveiliging van gezondheidsgegevens. Een verpleegster krijgt geen contractverlenging nadat verhalen over haar medische toestand rondgaan in het ziekenhuis waar ze werkte. Ze krijgt geen compensatie voor geleden schade door de Finse rechtbanken, aangezien deze bepalen dat zij niet kan aantonen dat er ongeautoriseerd toegang is verschaft tot haar medisch dossier. Het EHRM vindt het te ver gaan om van haar te vragen om het causale verband aan te tonen tussen de gebreken in de beveiligingsregels en de openbaarmaking van haar medische toestand. Het EHRM geeft daarbij aan dat zij niet in zo'n nadelige situatie hoeft terecht te komen indien het ziekenhuis een grotere mate van controle over toegang tot de gegevens verschaft, door de toegang te beperken tot de behandelaars en ook bij te houden wie toegang zoeken tot het dossier. Doorslaggevend voor het EHRM is dat het opslagsysteem niet voldoet aan de Finse wetgeving. Daarbij kunnen we volgens Herveg[465] van deze zaak leren dat de bescherming van het privéleven niet voldoende is wanneer er slechts de mogelijkheid is om schadevergoeding te claimen. Een praktische en effectieve bescherming is noodzakelijk waarbij de mogelijkheid van ongeautoriseerde toegang wordt uitgesloten.

461. Zoals in artikel 8 en 9 van het Verdrag van Straatsburg, en artikel 12 en 13 van richtlijn 95/46/EG wel het geval is.
462. Zie Achtergrondstudie ZonMW 2013.
463. EHRM 5 oktober 2006 (*Trocellier t. Frankrijk*).
464. EHRM 7 juli 2008 (*I. t. Finland*).
465. Herveg 2009.

In Codarcea t. Roemenië[466] is aan lidstaten de opdracht gegeven om een juridisch kader vast te stellen voor ziekenhuizen om de benodigde maatregelen te treffen om de bescherming van het privéleven van patiënten te verzekeren. Het Hof onderstreept ook het grote belang van de naleving van de nationale wetgeving ter bescherming van medische persoonsgegevens.

Het Hof is in de zaak M.S. t. Zweden[467] geconfronteerd met een zaak waarin medische informatie beschikbaar is gesteld aan sociale zekerheidsautoriteiten. Toch komt het Hof niet tot een schending, aangezien deze autoriteiten een wettelijke geheimhoudingsplicht hebben, en deze informatie daadwerkelijk nodig is voor de arbeidsgeschiktheidkeuringen die moesten worden uitgevoerd.

In Andersson t. Zweden[468] geeft een psychiater gezondheidsgegevens door aan sociale diensten. Dit wordt door het Hof gekwalificeerd als een inbreuk op artikel 8, lid 1, EVRM. Evenwel kan dit met een beroep op lid 2 worden gerechtvaardigd aangezien Andersson is geïnformeerd over de doorgifte van gegevens en haar gegevens niet aan het grote publiek zijn geopenbaard.

In de zaak Panteleyenko[469] heeft een Oekraïens Hof vertrouwelijke informatie van een psychiatrisch ziekenhuis opgevraagd en verkregen over de geestelijke gezondheidstoestand van de klager met betrekking tot haar medische behandeling. Vervolgens is deze informatie door het Hof gedeeld met de partijen en de overige aanwezigen bij de zitting. Dit is door het Hof aangemerkt als een inbreuk door een publieke autoriteit op artikel 8 EVRM. Deze inbreuk is als ongerechtvaardigd aangemerkt aangezien het Hof in Oekraïne de nationale regelgeving voor bescherming van psychiatrische gegevens niet had nageleefd en de gegevens niet van belang waren om tot een uitspraak te komen in de zaak.

In de zaak Gaskin[470] is het EHRM geconfronteerd met een klacht aangaande de weigering tot toegang tot een dossier. De psychiatrische patiënt Gaskin krijgt geen toegang tot zijn persoonlijke medische dossier. Het Hof oordeelt dat het dossier zonder twijfel informatie bevat met betrekking tot zeer persoonlijke aspecten van de jeugd, ontwikkeling en geschiedenis van de klager, en daarmee de belangrijkste bron van informatie over zijn verleden en vormende jaren vormt. Daarom is een gebrek aan toegang problematisch met betrekking tot artikel 8 EVRM. Het Hof maakt in het arrest een afweging tussen het publiek belang en het belang van het individu. Enerzijds is het belang van het individu om toegang te hebben tot alle persoonlijke informatie een relevant recht, en de Staat heeft daartoe ook een positieve verplichting voortvloeiend uit artikel 8 EVRM. Anderzijds is er een publiek belang om vertrouwelijke gegevens geheim te houden. In deze zaak acht het Hof artikel 8 EVRM geschonden omdat het recht

466. EHRM 2 juni 2009, ECLI:NL:XX:2009:BJ7513 (*Codarcea t. Roemenië*).
467. EHRM 27 augustus 1997, NJ 1999, 464 (*M.S. t. Zweden*).
468. EHRM 7 december 2010 (*Andersson t. Zweden*).
469. EHRM 29 juni 2006 (*Panteleyenko t. Oekraïne*).
470. EHRM, 7 juli 1989, Gaskin t. Verenigd Koninkrijk, NJCM-bulletin 1990, p. 206, https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjr9a3z2eLZAhVlJJoKHQOiBeQQFggoMAE&url=https%3A%2F%2Fwww.joho.org%2Fnl%2Fgaskin-vs-uk-ehrm-7-juli-1989-njcm-bulletin-1990-p-206-arrest&usg=AOvVaw1d5slNU0AdujAI7HtbaSjT.

op toegang niet is verzekerd in het Verenigd Koninkrijk. Het Hof vindt wel dat publieke autoriteiten inzage moeten kunnen weigeren in persoonlijke dossiers, maar daarbij moet het belang van het privéleven van de persoon nadrukkelijk worden afgewogen tegen het publieke belang. Een onafhankelijke autoriteit dient hier eventueel achteraf over te oordelen. De staten hebben een beoordelingsmarge om dit proces vorm te geven, maar in dit geval had het Verenigd Koninkrijk deze marge volgens het Hof overschreden.

In Z. t. Finland[471] gaat het om informatie met betrekking tot het HIV-virus dat Z. met zich meedraagt. Het Hof legt in dit arrest nog een strengere test op voor het openbaren van dergelijke gevoelige medische informatie, om te komen tot een gerechtvaardigde inbreuk op het recht op privacy. In het geval van strafzaken ziet het Hof nog een mogelijkheid om dergelijke gegevens te openbaren, maar daarbuiten zal over het algemeen vertrouwelijkheid prevaleren. In deze zaak komt het Hof tot de conclusie dat deze informatie wel in het belang van de rechtszaak openbaar mocht worden gemaakt. Tegelijkertijd rekent het Hof af met de Finse wet die het mogelijk maakt dat iedereen na tien jaar inzage krijgt in dergelijke gegevens. Daarbij geeft het Hof aan dat het in het algemeen noodzakelijk is dat nationale wetten genoeg waarborgen bieden om gevoelige gegevens, zoals ten aanzien van persoonlijke gezondheid, geheim te houden. De bescherming van slachtoffers en het algemeen belang kunnen onder omstandigheden gerechtvaardigde redenen zijn om het medisch beroepsgeheim te doorbreken.

In L.L. t. Frankrijk[472] wordt door het Hof verwezen naar het Verdrag van Straatsburg, waarin gezondheidsgegevens als persoonsgegevens zijn gedefinieerd. Het EHRM bepaalt dat het toelaten en gebruiken van medische documenten voor het bewijs in een rechtszaak een inbreuk betekenen op artikel 8 EVRM. In deze zaak gaat het om een scheiding. Bij een scheiding is het volgens het EHRM de plicht van een rechtbank om inbreuk te maken op de privésfeer van het stel, om daarmee de belangen van beide zijden goed te kunnen wegen. Toch moet deze inbreuk zo beperkt mogelijk blijven. Daarbij legt het EHRM de eis aan dat het gebruik van medische documenten alleen is toegestaan indien het noodzakelijk is om tot een uitspraak te komen.

In T.V. t. Finland[473] bepaalt het Hof dat het bekendmaken en doorgeven van informatie aan het gevangenispersoneel over de aidsbesmetting van een gevangene, een inbreuk is op artikel 8 lid 1 EVRM. Toch is dit gerechtvaardigd op grond van de bescherming van de openbare orde en het voorkomen van strafbare feiten. Daarbij is ook van belang dat geheimhouding stevig in de Finse wet is neergelegd en dat de informatie niet verder op onwettige wijze wordt verspreid.

471. EHRM 25 februari 1997 (*Z. t. Finland).*
472. EHRM 10 oktober 2006, nr. 7508/02, (*L.L. t. Frankrijk)*, *EHRC* 2006, 142 (m.nt. H.L. Janssen).
473. EHRM 12 maart 1994 (*T.V. t. Finland*).

Ingevolge het arrest Uslu[474] kunnen we stellen dat toegang tot gezondheidsgegevens onder het bereik van artikel 8 EVRM valt. Gezondheidsgegevens vallen onder het privéleven, en daarmee de toegang tot gezondheidsgegevens eveneens. In de zaak Uslu bepaalt het EHRM dat de klager een belang heeft bij het verkrijgen van een kopie van het rapport van de dokter die hem bezoekt in de gevangenis, alsmede de relevante bevestiging van de toegang tot de gevangeniskliniek. De klager krijgt deze documentatie niet, op basis van een circulaire van de minister van Justitie, waarin de gronden van veiligheid en algemene orde hiertoe werden aangevoerd. Deze gronden kunnen door het EHRM niet worden beschouwd als gerechtvaardigd om het belang van de klager te overstijgen om de documenten te krijgen. Het ontbreekt in dit geval aan een juridische basis en een specifieke reden om de documenten niet te geven. Het individuele belang was daarmee volgens het Hof niet goed afgewogen tegen het algemeen belang, wat leidt tot een schending van artikel 8 EVRM.

De zaak Szuluk[475] gaat om de bescherming van medische correspondentie. Er is een inbreuk op het recht op respect voor correspondentie wegens het controleren van de correspondentie van een veroordeelde gevangene met zijn medisch specialist van buiten de gevangenismuren. Of deze inbreuk op het privéleven gerechtvaardigd was moet door het Hof worden beoordeeld. Daarbij moet de normale gang van zaken in een gevangenis worden meegenomen, waarbij het Hof aangeeft dat enige mate van controle over de correspondentie van gevangenen geoorloofd is. Toch is in deze zaak, waarin de gevangene lijdt aan een levensbedreigende ziekte, de vertrouwelijkheid van correspondentie, volgens het Hof, van het grootste belang. De inbreuk op de medische correspondentie is daarom als ongerechtvaardigd beschouwd.

In K.H. et al.[476] is geklaagd over effectieve toegang tot informatie over gezondheid en reproductieve status. Het Hof ziet deze claim in relatie tot zowel privéleven als familieleven. Als het gaat om de toegang tot informatie dan heeft het Hof een positieve verplichting aan lidstaten gegeven om toegang te garanderen in bepaalde situaties. In Guerra[477] gaat het om toegang tot informatie over gezondheidsrisico's ten gevolge van milieuvervuiling, in de zaak McGinley en Egan[478] over de risico's van deelname aan nucleaire tests en in Roche[479] over een test waar sprake was van blootstelling aan giftige chemicaliën. Bij praktische en effectieve toegang tot informatie hoort volgens het Hof ook de mogelijkheid om kopieën van persoonlijke dossiers te kunnen krijgen.

5.5 RECHTSPRAAK HVJ-EU

Het Europees Hof van Justitie (HvJ-EU) heeft verscheidene uitspraken gedaan met betrekking tot de bescherming van persoonsgegevens. Aangaande de

474. EHRM 12 april 2007 (*Uslu t. Turkije*).
475. EHRM 2 juni 2009 (*Szuluk t. VK*).
476. EHRM 9 oktober 2007 (*K.H. et al t. Slowakije*).
477. EHRM 19 februari 1998 (*Guerra et al. t. Italië*).
478. EHRM 28 januari 2000 (*McGinley en Egan t. VK*).
479. EHRM 19 oktober 2005 (*Roche t. VK*).

bescherming van persoonsgegevens was richtlijn 95/46/EG betreffende de bescherming van persoonsgegevens tot 25 mei 2018 leidend in de jurisprudentie van het Hof. Nu is dat de AVG. Daarom wordt hieronder allereerst ingegaan op de betekenis en reikwijdte van deze richtlijn volgens het HvJ-EU. Vervolgens wordt beschreven hoe het Hof heeft geoordeeld over de botsing van het recht op bescherming van persoonsgegevens en het intellectueel eigendomsrecht. Het recht op bescherming van persoonsgegevens is ook in botsing gekomen met het recht op openbaarmaking van gegevens door de overheid, inzake de openbaarmaking van salarissen van personen die voor instanties onder overheidstoezicht werken. Vervolgens heeft het Hof een balans moeten vinden tussen enerzijds het belang van het bewaren van informatie en anderzijds de last van het bewaren van informatie, voor de instantie die hiervoor zorg moet dragen. Ten slotte wordt de zaak besproken waarin het Europees Parlement over het delen van persoonsgegevens van luchtvaartpassagiers met de Verenigde Staten tegenover de Europese Raad en de Europese Commissie stond.

5.5.1 Reikwijdte richtlijn 95/46/EG

Op 16 december 2008 doet het Hof een uitspraak waarin ze verschillende artikelen van de richtlijn betreffende bescherming van persoonsgegevens heeft geïnterpreteerd. Allereerst heeft ze uitleg gegeven aan het begrip 'verwerking van persoonsgegevens' dat gebruikt wordt in artikel 3 richtlijn 95/46/EG. Hiermee wordt de reikwijdte van de richtlijn bepaald. Verwerking van persoonsgegevens is volgens het Hof aan de orde wanneer gegevens over het inkomen en vermogen van natuurlijke personen door de fiscus worden verzameld en met het oog op openbaring bewerkt. Daarnaast is dit aan de orde wanneer deze gegevens in alfabetische volgorde en naar inkomenscategorie, in de vorm van uitvoerige, per gemeente gerangschikte lijsten, als drukwerk openbaar worden gemaakt. Of wanneer de gegevens op een cd-rom ter verwerking voor commerciële doeleinden worden verstrekt. Tenslotte valt onder verwerking van persoonsgegevens ook het gebruik van een sms-dienst. Het Hof geeft verderop in het arrest aan dat ook wanneer deze gegevens al in de media zijn gepubliceerd, dit toch onder het bereik van de richtlijn valt.

5.5.2 Lindqvist

De strekking van het arrest Lindqvist[480] van het HvJ-EU is dat het verwerken van gezondheidsgegevens is verboden. In het licht van richtlijn 95/46/EG oordeelde het HvJ-EU dat het publiceren van gezondheidsgegevens op een website verboden is, tenzij de verwerking valt onder de ontheffing van dit verbod. In het onderhavige geval, waarin de Zweedse mevrouw Lindqvist in het kader van een computercursus een website had ontwikkeld, is dat niet het geval. Dat betekent dat een dergelijke publicatie alleen mogelijk is, als de verwerking geschiedt met de uitdrukkelijke toestemming van de betrokkene.

480. HvJ EU november 2003, Zaak nr C-101/01 (*Lindqvist*).

5.5.3 Österreichischer Rundfunk e.a.

Een andere botsing van het recht op bescherming van persoonsgegevens is die met het recht op openbaarheid van overheidsinformatie. Hierover heeft het Hof in haar arrest van 20 mei 2003[481] een prejudiciële vraag beantwoord van Oostenrijkse hoven. Die vraag had direct betrekking op de richtlijn betreffende de bescherming van persoonsgegevens. En die vraag is door het Hof beantwoord in de context van de bescherming van grondrechten. Het Hof geeft in het arrest aan dat de bescherming van persoonsgegevens niet afhankelijk is van de vraag of de concrete situatie van een casus voldoende in verband staat met de uitoefening van de door het Verdrag beschermde fundamentele vrijheden.
Er is dus geen begrenzing van de bescherming van persoonsgegevens in die zin, zoals het Oostenrijkse Hof wel had bepaald. Het Hof geeft aan dat bij de uitleg van de richtlijn de grondrechten van belang zijn. Daarbij wijst het Hof op artikel 8 EVRM, het recht op privacy.

Het Hof geeft aan dat een werkgever wel gegevens mag opslaan van aan zijn personeel betaalde salarissen, maar dat hij dit niet aan een overheidsorgaan mag verstrekken, omdat dit afbreuk doet aan het recht op de persoonlijke levenssfeer. Daarbij maakt het weinig verschil of de meegedeelde gegevens al dan niet gevoelig zijn en of de betrokkenen nadeel hebben ondervonden. Wanneer het een controleorgaan van de Staat betreft dat gegevens over het inkomen van zijn werknemers moet verstrekken aan de Staat, dan kan inmenging in persoonsgegevens gerechtvaardigd zijn op grond van art. 8, lid 2, EVRM. Dat kan het geval zijn als de salarissen een bepaald maximum overschrijden en indien het noodzakelijk en passend is de salarissen binnen aanvaardbare grenzen te houden. Dit moet door de rechter worden beoordeeld.[482]

In Nederland valt bijvoorbeeld te denken aan de overheid die het salaris van bestuurders van woningcorporaties binnen bepaalde grenzen wil houden. Het is duidelijk dat in deze zaak de openbaarmaking van persoonlijke gegevens centraal staat, en het Hof geeft aan dat hier terughoudend mee moet worden omgegaan gezien het belang van privacy. Er wordt niet gesproken over zelfbeschikking ten aanzien van deze gegevens maar het Hof vindt wel dat de instanties die over persoonlijke gegevens beschikken, terughoudend moeten zijn wanneer het gaat om openbaarmaking. De Hert en Gutwirth[483] plaatsen kritische kanttekeningen bij deze uitspraak van het Hof. Ze signaleren dat het Hof slechts verwijst naar artikel 8 EVRM (bescherming van privacy) en niet naar artikel 8 Handvest (bescherming van persoonsgegevens). De beperkingen van artikel 8 EVRM ten aanzien van bescherming van persoonsgegevens zijn al eerder benoemd en komen hier terug. Het verstrekken van gegevens aan derden wordt in deze uitspraak aan voorwaarden gebonden, maar niet uitgesloten, zoals onder strikte bescherming van persoonsgegevens wel zou kunnen. Dat heeft volgens De Hert

481. HvJ EU 20 mei 2003, C-465/00 (*Österreichischer Rundfunk e.a.*).
482. Artikel 6, lid 1, sub c en artikel 7, sub c en e, van richtlijn 95/46/EG staan in ieder geval niet in de weg aan het treffen van een dergelijke nationale regeling in het kader van een goed beheer van de openbare middelen.
483. De Hert en Guthwirth 2009.

en Gutwirth ermee te maken dat het Hof de richtlijn 95/46/EG vanuit het perspectief van privacybescherming interpreteert.

5.5.4 Deutsche Telekom

De Deutsche Telekom zaak[484] heeft het Hof gesteld voor de vraag of het Europees recht eraan in de weg staat dat de Duitse Telecommunicatiewet verplichtingen oplegt aan ondernemingen die telefoonnummers toekennen. Het gaat om verplichtingen aan andere ondernemingen die openbare telefooninlichtingen of telefoongidsdiensten verstrekken. Daarbij stellen zij de gegevens van abonnees van derde ondernemingen waarover zij beschikken ter beschikking.

Artikel 12 van richtlijn 2002/58/EC gaat over gegevensbescherming en elektronische communicatie. Deze richtlijn bepaalt dat deze persoonsgegevens slechts kunnen worden doorgegeven indien de derde onderneming of haar abonnees daarvoor toestemming geven of daartegen geen bezwaar maken. Hier zien we het concept van informationele zelfbeschikking terug, aangezien het hier gaat om zelfbeschikking over openbaarmaking van persoonsgegevens. Alhoewel dit niet letterlijk in het arrest terugkomt. Op basis van artikel 8 Handvest en artikel 12 richtlijn 2002/58/EC komt het Hof tot de conclusie dat wanneer een abonnee voor de eerste keer aan een bedrijf als Deutsche Telekom toestemming geeft om de persoonsgegevens door te geven met het oog op de publicatie ervan in een openbare telefoongids van deze onderneming, het geen probleem is om diezelfde gegevens door te geven aan een andere onderneming die een openbare telefoongids beoogt te publiceren.

Er is dus geen nieuwe toestemming van de abonnees noodzakelijk, op voorwaarde dat de abonnees vóór de eerste opneming van hun gegevens in een openbare telefoongids op de hoogte zijn gebracht van het doel van deze gids en van het feit dat deze gegevens zouden kunnen worden meegedeeld aan een andere telefoondienstaanbieder. Ook moeten abonnees op de hoogte zijn van de waarborg dat deze gegevens na het doorgeven ervan, niet zullen worden gebruikt voor andere doeleinden dan die waarvoor zij met het oog op de eerste publicatie ervan zijn verzameld.
Het Europees recht staat daarmee niet in de weg van de Duitse wet die een onderneming van openbare telefoongidsen de verplichting oplegt om persoonsgegevens van abonnees van andere telefoondienstaanbieders, waarover zij beschikt, door te geven aan een derde onderneming van gedrukte of elektronische openbare telefoongidsen of ondernemingen die ervoor zorgen dat deze gidsen via inlichtingendiensten toegankelijk zijn.

5.5.5 Google Spain/Costeja

In het arrest Google Spain/AEPD and Mario Costeja González bepaalt het Hof in mei 2014 dat activiteiten van een zoekmachine zijn aan te merken als een

484. HvJ EU 5 mei 2011, Zaak C-543/09 (*Deutsche Telekom AG tegen Bundesrepublik Deutschland*).

verwerking van persoonsgegevens.[485] Een zoekmachine vindt informatie die leidt tot geïdentificeerde of identificeerbare natuurlijke personen. Die informatie wordt verzameld, opgevraagd, vastgelegd, geordend, ter beschikking gesteld, verstrekt en op een server bewaard. Google stelt het doel en de middelen van deze activiteiten vast. Google is dus de verantwoordelijke voor de koppeling naar de gepubliceerde webpagina's. Zij het dat de exploitant van de zoekmachine alleen verantwoordelijk is voor het vinden. Over de inhoud moet de betrokkene bij de webredacteur zijn. Google Spain is de verantwoordelijke voor het vinden van de informatie en dus voor de verwerking van persoonsgegevens via de zoekmachine. Een verzoek tot wijziging of correctie van de link dient derhalve aan Google gericht te worden.

Voor de rechtmatigheid van de verwerking is niet slechts van belang of de verwerkte gegevens onjuist of onvolledig zijn, maar ook of de verwerking anderszins verenigbaar is met de bepalingen van richtlijn 95/46/EG. Daarbij moet, aldus het Hof, onder meer gedacht worden aan de vereisten met betrekking tot het doel van de verwerking en het verbod van bovenmatige verwerking.[486] Vervolgens formuleert het Hof nog de hoofdlijnen voor de conflicterende grondrechten:
'Tussen het privacybelang van degene die zijn gegevens verwijderd wil zien en anderzijds de gerechtvaardigde belangen van de internetgebruikers die toegang tot de informatie willen krijgen en het belang van de exploitant van de zoekmachine dient een juist evenwicht te worden gevonden.'
Bovendien wordt opgemerkt dat de gezochte persoon op internet extra bescherming behoeft. De inmenging is des te sterker, aldus het Hof, door de belangrijke rol die internet en zoekmachines in onze moderne samenleving spelen. De informatie in een resultatenlijst op grond van een zoekopdracht is ook overal beschikbaar.

De betrokkene kan op basis van zijn door de artikelen 7 en 8 Handvest gewaarborgde grondrechten verlangen dat de informatie in een resultatenlijst op grond van een zoekopdracht niet meer ter beschikking wordt gesteld. Deze rechten krijgen, zoals met name blijkt uit overweging 81 van het onderhavige arrest, in beginsel voorrang. Deze rechten krijgen niet enkel voorrang op het economische belang van de exploitant van de zoekmachine, maar ook op het belang om deze informatie te vinden, wanneer op naam van deze persoon wordt gezocht.'
In dit geval valt dus, vanwege de bijzonderheid van de verkregen informatie door de zoekmachine, de '*fair balance*' uit in het voordeel van de gegevensbeschermingsrechten van de betrokkene. Maar dat zal niet altijd het geval zijn. Het Hof stelt uitdrukkelijk:

> *"Dit zal echter niet het geval zijn indien de inmenging in de grondrechten van de betrokkene wegens bijzondere redenen, zoals de rol die deze persoon in het openbare leven speelt, wordt gerechtvaardigd door het overwegende belang dat het publieker bij heeft om door deze opneming, toegang tot de betrokkene informatie te krijgen."*[487]

485. HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (GoogleSpain/Costeja).
486. R.o. 81.
487. R.o. 97.

Hier dient dus nog een belangenafweging plaats te vinden. Kortom: conflicterende grondrechten verdienen een '*fair balance*', maar bij verkregen informatie uit zoekmachines en het grote belang daarbij van de betrokkene gaan gegevensbeschermingsrechten voor, tenzij zich bijzondere redenen voordoen. In geval van bijzondere redenen zal dan nog wel een belangenafweging met de belangen van betrokkenen dienen plaats te vinden.

5.5.6 Uitwisseling luchtvaartpassagiersgegevens VS

Een zaak[488]die veel aandacht trok was die waarin het Europees Parlement tegenover de Europese Raad en de Europese Commissie stond, vanwege de beslissing om persoonsgegevens van luchtvaartpassagiers te delen met de Verenigde Staten. Het Parlement achtte dit besluit namelijk in strijd met de richtlijn inzake bescherming van persoonsgegevens, richtlijn 95/46/EG. Daarom was het Parlement het ook oneens met de beslissing van Raad en Commissie om het besluit inzake het delen van persoonsgegevens van luchtvaartpassagiers naar de Verenigde Staten, uit te sluiten van de reikwijdte van de richtlijn.[489] Volgens het Hof is daarbij de rechtsgrondslag het probleem van de overeenkomst, en niet de gegevensbescherming die van de richtlijn uitgaat. Inhoudelijk geeft het Hof namelijk juist aan dat in het kader van de openbare veiligheid en de strafrechtspleging deze verwerking van persoonsgegevens buiten de reikwijdte van de richtlijn, en daarmee ook buiten de geboden bescherming van de Richtlijn valt. Dat is niet de intentie waarmee het Parlement de besluiten van de Raad en de Commissie ongeldig wil verklaren, aangezien zij de overeenkomst met de Verenigde Staten inhoudelijk in strijd achtten met de richtlijn. Het Hof laat daarmee de gebreken zien van de gegevensbescherming van Richtlijn 95/46/EG.

5.5.7 Dataretentiearrest

Ook invloedrijk was het Dataretentiearrest[490], dat hierna is uitgewerkt. Op 8 april 2014 heeft het HvJ-EU – in lijn met de in hoofdstuk 4 aangehaalde Duitse rechtspraak over de Dataretentierichtlijn – een opzienbarend arrest over de Dataretentierichtlijn uitgesproken waarbij het Hof het grondwettelijke recht op privacy en de bescherming van persoonsgegevens als uitgangspunt heeft genomen.

Door Oostenrijkse en Ierse rechters zijn prejudiciële vragen gesteld aan het Hof van Justitie in Luxemburg over de rechtsgeldigheid van de Dataretentierichtlijn 2006/24. Op grond van die richtlijn moeten telecombedrijven verkeers- en locatiegegevens van al hun klanten tussen de zes maanden en twee jaar bewaren. Het Hof onderzoekt de geldigheid van de richtlijn aan de hand van artikel 7 en 8 van het EU Grondrechtenhandvest. Eerst wordt vastgesteld dat de richtlijn een verrijkende en bijzonder serieuze inbreuk maakt op het recht

488. HvJ EU 30 mei 2006, C-317/04 (*Uitwisselingluchtvaartpassagiersgegevens VS*).
489. Het Hof geeft het Parlement daarin gelijk en bepaalt dat het besluit niet geldig tot stand is gekomen op basis van artikel 25 richtlijn 95/46/EG.
490. HvJ EU 8 april 2014, C-293/12 en C-594/12 (*Digital Rights Ireland en Seitlinger*).

op privacy en gegevensbescherming. Vervolgens stelt het Hof vast dat het doel van de richtlijn, het bestrijden van zware misdaad en de bescherming van de openbare orde, legitiem is. Het Hof beoordeelt daarna of de inbreuk proportioneel is met het oog op het doel van de richtlijn. De beleidsvrijheid van de lidstaten wordt in dit geval klein geacht, gezien de belangrijke rol die persoonsgegevens spelen bij het recht op bescherming van de persoonlijke levenssfeer en de omvang van de inperking van dat recht. Het Hof benadrukt dat de bestrijding van zware misdaad, hoe fundamenteel dat ook moge zijn, niet op zichzelf een inbreuk op de grondrechten rechtvaardigt die door de richtlijn noodzakelijk voor dat doel wordt geacht.

Ook wordt gesteld dat de richtlijn praktisch inbreuk maakt op de grondrechten van de gehele Europese bevolking, omdat het een bewaarplicht oplegt voor alle verkeersgegevens betreffende vaste en mobiele telefonie en al het internetverkeer. De richtlijn beïnvloedt zonder uitzondering iedereen die elektronisch communiceert, ook personen bij wie geen bewijs is dat er zelfs maar een verre link bestaat met enige zware misdaad. Bovendien worden er geen uitzonderingen gemaakt voor personen die volgens de wet verplicht zijn tot geheimhouding, zoals artsen. Verder stelt de richtlijn geen beperkingen aan toegang tot en gebruik van de gegevens en wordt niet vereist dat de nationale keuzes voor de lengte van de bewaartermijn worden onderbouwd. Tot slot worden onvoldoende waarborgen gegeven voor de beveiliging van gegevens. Het Hof concludeert daarom dat de richtlijn als geheel ongeldig is.

5.5.8 Schrems t. Facebook

Nog verder strekt de invloed van de zaak van Schrems tegen de Ierse Data Protection Authority inzake Facebook.[491] Die heeft geleid tot beëindiging van het Safe Harbour Agreement[492] op grond waarvan persoonsgegevens vanuit Europa naar de VS mochten. Facebook-gebruikers binnen de EU hebben formeel een overeenkomst met Facebook Ireland, een dochteronderneming van Facebook Inc. Die laatste is gevestigd in de VS. Schrems is een Oostenrijkse burger die mede naar aanleiding van de 'Snowden Revelations' omtrent verregaande overheidssurveillance door de NSA een klacht indiende tegen het doorsturen van zijn gegevens naar servers in de VS bij de Ierse dataautoriteit, de 'Commissioner', wat uiteindelijk heeft geleid tot een rechtszaak die bij het Hof is geëindigd. Het geschil spitste zich toe op de vraag of de EC in beschikking 2000/520 terecht had gesteld dat het recht in de VS 'passende bescherming' biedt voor persoonlijke gegevens, hetgeen een voorwaarde was voor de rechtmatigheid van het delen van persoonsgegevens buiten de EU op grond van Richtlijn 95/46/EG. De VS en de EU hadden hiervoor een aparte afspraak gemaakt.[493]

Het Hof zette vraagtekens bij het mechanisme van zelfcertificering waarbij het Hof onvoldoende duidelijk vond hoe de betrouwbaarheid van deze certificaten

491. HvJ 6 oktober 2015, zaak C-362/14, Facebook/Schrems, ECLI:EU:C:2015:650.
492. Beschikking 2000/520/EG, PbEG 2000, L 215/7.
493. Het zogenoemde "Safe harbour Agreement".

werd gecontroleerd. De vraag was ook of gezien de feiten omtrent brede overheidssurveillance, onder andere via het PRISM-programma van de NSA, met deze constructie wel voldaan is aan de vereiste van passende bescherming omtrent het doorgeven van persoonsgegevens aan derde landen, het Hof vond deze bevoegdheden onvoldoende met waarborgen omkleed. Verder mist het Hof klachtenprocedures en mogelijkheid voor burgers om in bezwaar en beroep te komen.[494]

Vervolgens begonnen de Europese Commissie en de VS onderhandelingen over het *Privacy Shield*[495] als vervanging van *Safe Harbour*. Het *Privacy Shield* wordt nog geëvalueerd.[496] De Oostenrijker Schrems wil Facebook via een rechtszaak bij het Hof collectief aanvechten via een '*class-action*'. Het *Oberste Gerichtshof* (hoogste federale rechter in civiele en strafzaken in Oostenrijk) heeft het Hof om een prejudiciële beslissing gevraagd in deze zaak.[497] Advocaat-generaal Bobek van het Hof heeft op 14 november 2017 in een advies aan dit Hof geoordeeld dat Schrems dit niet collectief kan doen namens 25.000 anderen, omdat een dergelijke zaak volgens Oostenrijks recht alleen kan als een Oostenrijks bedrijf wordt aangesproken. Een collectieve zaak is niet mogelijk als een Oostenrijkse consument een bedrijf in een andere EU-lidstaat aanklaagt. Volgens Bobek kan iemand die in staat is om een buitenlandse partij in zijn eigen land aan te klagen voor zijn eigen belangen, niet ook nog eens tegelijk een zaak starten voor een hele groep.[498]

Het Hof[499] heeft 25 januari 2018 geoordeeld dat Schrems moet worden gezien als consument, wat betekent dat hij in zijn thuisland, Oostenrijk, een zaak kan aanspannen tegen Facebook. Het Amerikaanse bedrijf was van mening dat Schrems als bedrijf moet worden gezien, omdat hij in een professionele hoedanigheid gebruikmaakt van het sociale netwerk door een eigen Facebook-pagina te hanteren. Het Hof gaat hier niet in mee en zegt dat activiteiten als het inzamelen van giften en exploiteren van websites niet tot gevolg heeft dat hij de status van consument verliest. Het Hof zegt echter ook dat Schrems niet namens anderen een zaak in Oostenrijk kan beginnen.

5.5.9 Zelfbeschikking van patiënten

Het HvJ-EU heeft zich ook al eens uitgelaten over het recht op zelfbeschikking van patiënten en deze erkend, zij het dat hier niet om 'informationele' zelfbe-

494. Beschikking 2000/520 was daarmee in strijd met het Unierecht, waaronder het EU-handvest en de Commissie Handelde dus buiten haar bevoegdheid, wat leidde tot de nietigheid van deze beschikking en daarmee effectief een einde aan Safe Harbour.
495. COM(2016)117 final, 29 Februari 2016.
496. Press release, *EU-U.S. data flows and data protection: opportunities and challenges in the digital era -- Speech at the Center for Strategic and International Studies by Věra Jourová, Commissioner for Justice, Consumers and Gender Equality,* Washington, 31 March 2017.
497. Zaak C-498/16 'Maximilian Schrems tegen Facebook Ireland Limited'.
498. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d63d5de6af03c8452e9316aa90e2102c5d.e34KaxiLc3qMb40Rch0SaxyMc3r0?text=&docid=196628&pageIndex=0&doclang=NL&mode=lst&dir=&occ=first&part=1&cid=552873.
499. https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-01/cp180007nl.pdf.

schikking ging.[500] De EU heeft slechts beperkte bevoegdheid over gezondheid, waardoor er minder jurisprudentie over dit onderwerp bij de EU is dan bij het EHRM. Het gaat hier om zelfbeschikking in het algemeen als onderliggend beginsel voor het gezondheidsrecht.[501]

5.6 CONCLUSIE EUROPA

Op Europa niveau is zowel de bescherming van privéleven als van persoonsgegevens verankerd. Artikel 8 EVRM en artikel 7 EU-Handvest beschermen het privéleven. Het Verdrag van Straatsburg, artikel 8 EU-Handvest en de AVG beschermen persoonsgegevens.

Artikel 8 EVRM reikt minder ver dan het recht op informationele zelfbeschikking vanwege een andere beperkingssystematiek dan de beperkingssystematiek van grondrechten door het Duits Constitutioneel Hof dat een stevigere proportionaliteitstoets aanlegt dan gebruikelijk is volgens het EVRM.
Nissenbaum bekritiseert de dominante, juridische denkwijze om het recht op privacy te zien als een recht op controle op informatie en het recht op geheimhouding. Zo'n rigide definitie leidt tot een recht dat niet te verdedigen valt, omdat er alleen maar uitzonderingen op bestaan.

Artikel 8 EVRM blijkt tekortkomingen te hebben in het licht van het groeiende gebruik van informatietechnologie in het algemeen en de opmars van persoonlijke gezondheidsomgevingen in het bijzonder. Misbruik van persoonsgegevens door private organisaties valt bijvoorbeeld niet onder de reikwijdte van 'privéleven' in artikel 8 EVRM. Het Verdrag van Straatsburg, het EU-Handvest en de AVG bieden wel die bescherming.

In de AVG is een aantal afzonderlijke 'informationele zelfbeschikkingsrechten' uitgebreid. Voorbeelden hiervan zijn het recht op elektronische inzage en het recht op dataportabiliteit. Voor persoonlijke gezondheidsomgevingen is het recht op dataportabiliteit in artikel 20 AVG 'slechts' van toepassing voor zover gegevens in een medisch dossier of persoonlijke gezondheidsomgeving door de betrokkene zelf zijn verstrekt aan de zorgaanbieder of de leverancier van een persoonlijke gezondheidsomgeving. Dit nieuwe recht is een stimulans voor het tot stand komen van persoonlijke gezondheidsomgevingen, omdat het succes hiervan staat of valt met de mogelijkheid om gegevens over te dragen. Bij een recht op dataportabiliteit voor alle gegevens in een medisch dossier of persoonlijke gezondheidsomgeving van de betrokkene zou de ontwikkeling van persoonlijke gezondheidsomgevingen nog meer bijdragen aan informationele zelfbeschikking. Het gaat om een nieuw recht waar nog ervaring mee moet worden opgedaan. Mocht in de praktijk blijken dit nieuwe recht – door de beperking dat het alleen om tot door de betrokkene zelf verstrekte gegevens gaat – de ontwikkeling van informationele zelfbeschikking via persoonlijke gezondheids-

500. HvJ EU 9 oktober 2001, C-377/98, (*Nederland t. Parlement en Raad*).
501. HvJ EU 5 oktober 1994, zaak C-404/92, (*X t. Commissie), zie ook:* HvJ EU 5 mei 2011 Zaak C-316/09, (*MSD Sharp & Dohme GmbH/Merckle GmbH*) waarin gesproken wordt van 'zelfbestemmingsrecht'.

omgevingen teveel belemmeren, dan valt wetgeving te overwegen om de reikwijdte van artikel 20 AVG te verruimen. Overigens is ook geconstateerd dat het – beperkte – recht op dataportabiliteit daarnaast juist ook bijdragen aan het misbruik van persoonlijke gezondheidsomgevingen bij bijvoorbeeld kwetsbare personen indien er geen aanvullende waarborgen zijn.

De scope van de AVG omvat ook bedrijven die op de Europese markt opereren vanuit een vestiging elders in de wereld. Voor de markt van persoonlijke gezondheidsomgevingen, via apps en smartphones, kan dit van groot belang zijn, omdat veel van de aanbiedende bedrijven zich buiten de EU bevinden.

Rouvroy en Poullet kritiseren de formulering van het tweede lid van artikel 8 EU-Handvest over bescherming van persoonsgegevens, waarin wordt gesuggereerd dat toestemming een voldoende legitieme grond voor gegevensverwerking is. Hun kritiek op toestemming als mogelijke grondslag om persoonsgegevens te verhandelen komt overeen met het eerdere pleidooi van Jacobs om het commercieel exploiteren van 'eigen' medische gegevens te verbieden.

Het Europees Hof van Justitie heeft verscheidene uitspraken gedaan met betrekking tot de bescherming van persoonsgegevens. Het meest verstrekkend en actueel is de invloed van de zaak Schrems tegen Facebook. Die heeft geleid tot beëindiging van het *Safe Harbour Agreement*. Op dit moment bereidt Schrems – als consument – vanuit zijn thuisland Oostenrijk een zaak voor tegen Facebook en het *Privacy Shield* als vervanging van *Safe Harbour*.

6. *Nederland*

6.1 INLEIDING

In de vorige hoofdstukken is voor Duitsland en Europa antwoord gegeven op de eerste onderzoeksvraag van deze dissertatie:

> In hoeverre is informationele zelfbeschikking mogelijk en wenselijk, met welke beperkingen? Kan en moet daarbij onderscheid worden gemaakt naar typen personen?

In dit hoofdstuk wordt deze vraag specifiek beantwoord voor Nederland en tevens een antwoord gegeven op de tweede onderzoeksvraag:

> Wat betekent een en ander concreet voor de uitwerking van informationele zelfbeschikking via regulering in Nederland?

De uitspraak over informationele zelfbeschikking van de Europese rechter Petitti in de zaak Malone[502] werkt rechtstreeks door in Nederland. Dit hoofdstuk gaat eerst in op de dogmatiek in Nederland. Vervolgens komt de relevante regulering aan bod. Ten eerste artikel 10 Grondwet. Daarna de Nederlandse Uitvoeringswet UAVG[503]. In het vorige hoofdstuk, paragraaf 5.3.7, kwam de AVG[504] en al aan de orde. De AVG en de UAVG hebben 25 mei 2018 de Richtlijn 95/46/EG[505] en de Wbp vervangen. Na de UAVG volgt de relevante gezondheidsrechtelijke regulering die invulling geeft aan informationele zelfbeschikking.

502. Zie paragraaf 5.5.1.
503. Als uitgangspunt is het gewijzigde wetsvoorstel UAVG dat 13 maart 2018 door de Tweede Kamer is aangenomen en 14 maart 2018 bij de Eerste Kamer is ingediend. Kamerstukken I, 2017-2018, 34 851, nr.B. De AP heeft door wijziging van het wetsvoorstel UAVG in de Tweede Kamer op 9 maart 2018 rechtspersoonlijkheid gekregen. Daarnaast heeft de Tweede Kamer 13 maart bij het aannemen van het wetsvoorstel UAVG tevens onder andere de motie 'hulpvaardige handhaving' aangenomen. De strekking van die motie is dat de AP zowel een handhavingstaak als een voorlichtingstaak heeft, met het verzoek aan de AP in de fase waarin nog veel vragen zijn over de regels, zich primair te richten op voorlichting en hulp bij de interpretatie en uitvoering van de regelgeving, onverlet haar handhavingstaak inzake bewuste schendingen. Zie: https://zoek.officielebekendmakingen.nl/dossier/34851/kst-34851-18?resultIndex=10&sorttype=1&sortorder=4.
504. Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). *PbEU* L 119.
505. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van gegevens. PbEG 1995 L 281/31.

In het licht van de eerste en tweede onderzoeksvraag staat in dit hoofdstuk de vraag centraal in hoeverre de Nederlandse regulering voldoende anticipeert op maatschappelijke en technologische ontwikkelingen rond informationele zelfbeschikking in de zorg. Bijvoorbeeld wat betreft regulering die rekening houdt met de in opkomst zijnde persoonlijke gezondheidsomgevingen. In hoeverre kan geanticipeerd worden op de machtsverschuiving ten aanzien van de beschikking over gezondheidsgegevens naar partijen buiten de (geneeskundige) behandelrelatie, in een tijdperk van nieuwe technologieën?[506]

6.2 NEDERLANDSE REGULERING

Het eerder besproken Duitse en Europese recht heeft invloed op het Nederlandse rechtssysteem. In het Nederlandse staatsrecht geldt een zogenoemd gematigd monistisch stelsel[507]. Alleen 'ieder verbindende bepalingen' uit internationale verdragen werken rechtstreeks door. Voor Europees recht ligt dit anders omdat het EU-verdrag een supranationale rechtsorde initieert.[508]

Alhoewel de uitwerking en toepassing van het Duitse en Europese recht zich niet zomaar laten transponeren naar de Nederlandse rechtsorde, zijn bepaalde elementen wel degelijk in de Nederlandse context in te brengen. Een aanknopingspunt voor deze redenering biedt het algemeen persoonlijkheidsrecht. In Nederland is het algemeen persoonlijkheidsrecht net als in Duitsland niet gecodificeerd maar wel in de rechtspraak benoemd.[509]

6.2.1 Artikel 10 Grondwet

In paragraaf 5.2 over het Europese begrip 'privacy' – preciezer 'privéleven' – kwam aan de orde dat net als bij het Amerikaanse privacyrecht, ook in Nederland de uitvinding van de draagbare fotocamera een belangrijke rol speelt in de eerste literatuur waarin aandacht werd besteed aan de bescherming van de persoonlijke levenssfeer. Namelijk de literatuur van De Brauw en Van Veen in hun preadviezen voor de Nederlandse Juristen Vereniging (NJV) in 1965.[510] Op het preadvies waren de foto's van invloed die fotojournalist John de Rooy op 1 mei 1965 met telelens maakte van prinses Beatrix en Claus von Amsberg, in de tuin van Drakesteyn.[511] Dit preadvies is gebruikt als voorstudie voor de uitbreiding van de strafrechtelijke bescherming tegen het heimelijk afluisteren, opnemen en doorgeven van (telefoon)gesprekken, het aanprijzen, plaatsen en doorgeven van afluisterapparatuur en het heimelijk maken van foto's (art. 139a

506. Zoals *big data* en de zogenaamde NIBC-covergence: het op dit moment samenkomen en vervloeien van vier belangrijke technologieën: nano, bio, informatie en cognitie. De Mul (2016) noemt dit versmeltende technologieën, omdat ze niet alleen versmelten met elkaar, maar ook met de (organische) mens.
507. Artikel 93 Grondwet: Bepalingen van verdragen en van besluiten van volkenrechtelijke organisaties, die naar haar inhoud eenieder kunnen verbinden, hebben verbindende kracht nadat zij zijn bekendgemaakt.
508. Van der Pot 2006, p. 272-273.
509. HR 15 april 1994, NJ 1994, 608 (Valkenhorst); Nehmelman 2002; Nieuwenhuis 2001.
510. De Brauw, 1965.
511. Henri Beunders en Herman Setier, Hoe een gearmd stel Het Paar werd in de Volkskrant van 29 april 1995.

e.v. en art. 441a en 441b Wetboek van Strafrecht (Sr)) bij wet van 7 april 1971, Stb. 1971, 180.

In Duitsland en Nederland vormden in de jaren zeventig vervolgens de volkstelling – gefaciliteerd door computersystemen[512] – aanleiding om wettelijk verankerde grenzen te trekken voor privacy en het grootschalig verzamelen van persoonsgegevens met de bijbehorende waarborgen om die persoonsgegevens te beschermen. Het privacyconcept heeft zich onder invloed van technologische innovaties – zoals fotografie, computer en internet – ontwikkeld vanuit het huisrecht naar een meer immaterieel georiënteerd aanknopingspunt met telkens nieuwe privacyvraagstukken.[513] Dit is een vorm van negatieve bescherming van de privésfeer, waarin anderen niet mogen binnendringen.[514]

Het recht op bescherming van de persoonlijke levenssfeer is sinds 1983 in artikel 10 van de Nederlandse Grondwet opgenomen. De regering gaf in de memorie van toelichting bij het Grondwetswijzigingsvoorstel de volgende toelichting:

> *"De termen 'persoonlijke levenssfeer' en 'privacy' wekken de indruk een gebied aan te duiden waarbinnen elk individu vrij is en geen inmenging van anderen behoeft te dulden."*[515]

Verder wordt in dezelfde Grondwetsgeschiedenis melding gemaakt van betekenissen als:

> *"Het recht zijn eigen leven te leiden met zo weinig mogelijk inmenging van buitenaf' en 'de reeks van situaties waarin de mens (…) onbevangen zichzelf wil zijn'."*

Volgens Verhey lijkt zelfbeschikking impliciet aan artikel 10 Grondwet ten grondslag te liggen. Hij geeft echter ook aan dat het begrip 'zelfbeschikking' vooral in gezondheidsrechtelijke context tot ontwikkeling is gekomen en gehanteerd wordt, terwijl daarbuiten vaak eerder over het 'persoonlijkheidsbeginsel' of 'zelfontplooiing' wordt gesproken.[516]

Belangrijk is verder dat in de praktijk artikel 10 Grondwet wordt beschouwd als een algemeen recht, waarvan de lichamelijke zelfbeschikking in artikel 11 Grondwet een *specialis* vormt:[517] '*Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van het lichaam*'. Aangezien er weinig persoonlijker is dan het eigen lichaam, kan de lichamelijke integriteit worden opgevat als een kernelement van de persoonlijke levenssfeer[518], zoals op meerdere plaatsen in de totstandkomingsgeschiedenis van artikel 11 is te lezen. Op een vergelijkbare wijze wordt de lichamelijke integriteit in de systematiek van het EVRM in de eerste plaats beschermd door het in artikel 8 EVRM neergelegde

512. Zie bijvoorbeeld Hustinx 1973, p.11, die spreekt over de vrijheid om de persoonlijkheid te ontplooien bij de toepassing van de computer.
513. Moerel & Prins 2016, p. 35.
514. Zie de negatieve vrijheid van Berlin in 3.5.
515. MvT bij het voorstel om een aantal grondrechten in de Grondwet op te nemen, Kamerstukken II, 1975-1976, 13 872, nr. 1-5, p. 41. Zie ook Achtergrondstudie ZonMw 2013, 4.3.
516. Verhey, 1992, p.207 en volgende.
517. Van Beers 2009, p. 126.
518. Kamerstukken II, 1979-1980, 16 086, nr. 8, p. 1-2.

recht op respect voor privéleven. Volgens vaste Straatsburgse jurisprudentie moet onder de term 'privéleven' mede worden begrepen '*the physical and moral integrity of the person.*'[519]

Nederland is samen met Duitsland één van de weinige landen die de lichamelijke integriteit afzonderlijk en uitdrukkelijk constitutioneel heeft vastgelegd. In tegenstelling tot bijvoorbeeld internationaal recht, namelijk het EVRM, waarin het recht op lichamelijke integriteit slechts als onderdeel van het recht op privéleven[520] en van het martelverbod wordt erkend. In Nederland kreeg destijds de lichamelijke integriteit een *status aparte* in de Grondwet dankzij een amendement van VVD-kamerlid Kappeyne van de Coppelo.[521] De gedachte achter een zelfstandige positivering van het recht op lichamelijke integriteit was om, hoewel het volgens de regering wel degelijk behoort tot het recht op de persoonlijke levenssfeer, op die manier 'onzekerheid over de grondwettelijke bescherming van dit recht op te heffen'.[522] Uit de formulering '*onaantastbaarheid van het lichaam'* valt indirect de noviteit van dit grondrecht voor de Nederlandse rechtsorde af te leiden. Ten tijde van de introductie van dit grondrecht zag de grondwetgever zich genoodzaakt ter inspiratie uit te wijken naar de Duitse rechtsdogmatiek en jurisprudentie.[523] Het fluorideringsarrest[524] werd door Kappeyne van de Coppello als een van de voornaamste aanleidingen van haar wetsvoorstel gezien. Verder blijft de jurisprudentie van voor die tijd beperkt tot een handvol uitspraken.[525] Artikel 11 Grondwet lijkt een vertaling van de Duitse formulering van het recht, namelijk het in artikel 2 II GG vastgelegde *Recht auf körperliche Unversehrtheit*.[526]

Artikel 11 Grondwet heeft eveneens betrekking op de relatie tussen hulpverlener en patiënt. Dit artikel ligt – wat betreft de lichamelijke zelfbeschikking – ten grondslag aan de wettelijke regeling van de geneeskundige behandelingsovereenkomst, de WGBO. In subparagraaf 6.2.3 komt de WGBO aan de orde voor wat betreft informationele zelfbeschikking. Er is veel rechtspraak over informatieverplichtingen en informatierechten. In relatie tot artikel 11 Grondwet is in het bijzonder de uitspraak van de Hoge Raad in het Dwarslaesie-arrest illustratief. In deze uitspraak wordt uit artikel 11 afgeleid dat een arts verplicht is zijn patiënt op duidelijke wijze in te lichten over de mogelijke risico's van een medische behandeling, zodat de patiënt een weloverwogen beslissing kan nemen of hij hier al dan niet zijn toestemming voor verleent.[527]

Privacy en gegevensbescherming 'wortelen' in oudere negentiende-eeuwse klassieke grondrechten (de afweerrechten, gelijkheidsrechten en participatie-

519. EHRM 26 maart 1985, NJ 1985, 525, m.nt. E.A. Alkema (*X en Y t. Nederland*).
520. Zie de hiervoor genoemde vaste Straatsburgse jurisprudentie, zoals EHRM 26 maart 1985 X en Y t. Nederland.
521. Van Beers, p. 111.
522. Handelingen II, 1979-1980, 16 086, nr. 8, p.1-2.
523. Handelingen II, 1978-1979, 15 463, nr.2, p.4.
524. HR 22 juni 1973, NJ 1973, 386 (Fluoridering).
525. Een overzicht van deze uitspraken is te vinden in Kors 1981.
526. Kors, 1981, p. 107.
527. HR 23 november 2001, NJ 2002, 386 en 387, m.nt. Vranken, r.o. 3.5.2 (Dwarslaesie).

rechten in de artikelen 1 tot en met 18 Grondwet) en in de lange traditie van het medisch beroepsgeheim. Evenals de lichamelijke integriteit beschermen ook het huisrecht[528] en het briefgeheim[529] specifieke aspecten van de persoonlijke levenssfeer. Er is niet veel bekend over de precieze betekenis van artikel 10 Grondwet voor de invulling van de notie van informationele zelfbeschikking in het algemeen en in het gezondheidsrecht in het bijzonder.

In de praktijk is de grondrechtelijke bescherming die in het kader van artikel 10 Grondwet wordt geboden, in samenspel met artikel 8 EVRM, verstrekkend. Vanwege dat samenspel met artikel 8 EVRM is in de literatuur impliciet uit artikel 10 Grondwet informationele zelfbeschikkingafgeleid, dat beschermt tegen de ongeautoriseerde verwerking van persoonsgegevens.[530] De Staatscommissie Grondwet heeft in 2010 zelfs voorgesteld dit recht in een zelfstandige Grondwetsbepaling vast te leggen.[531] Een zelfstandige Grondswetsbepaling voor informationele zelfbeschikking is vooralsnog niet in zicht en er is ook kritiek op dit voorstel.[532] Bovendien is het de vraag of een Grondswetbepaling voor informationele zelfbeschikking nog relevant is nu dit hele domein dwingend EU-recht is. Hijmans wijst in navolging van de Raad van State op het afnemend belang van artikel 10 lid 2 en 3 Grondwet, die regelingsopdrachten bevatten voor de nationale wetgever op het terrein van de bescherming van persoonsgegevens. Hijmans stelt naar mijn oordeel terecht dat artikel 10, lid 2 en 3 een dode letter is geworden, behoudens terreinen waar het EU-recht niet van toepassing is.[533] Het EU-recht is volgens de memorie van toelichting op de UAVG bijvoorbeeld niet van toepassing op het Caribische deel van Nederland. Daar geldt de Wet bescherming persoonsgegevens BES (Bonaire, St. Eustatius en Saba).[534]
Op grond van artikel 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU) stelt de Europese wetgever de regels. De uitputtende formulering van artikel 16 laat geen ruimte voor autonome nationale wetgeving.[535] Dit neemt niet weg dat de AVG in een aantal situaties expliciet ruimte laat voor nationale wetgeving.[536] De nationale wetgeving is dan echter niet gebaseerd op artikel 10 van de Nederlandse Grondwet, maar op artikel 16 VWEU en de AVG.

Hoewel artikel 10, lid 2 en 3 Grondwet inmiddels een vrijwel dode letter is geworden door het dwingend EU-recht, is voor de rechtsontwikkeling in Neder-

528. Artikel 12 Grondwet.
529. Artikel 13 Grondwet.
530. Overkleeft-Verburg 2000, p. 177. Zie ook HR 2 december 1988, NJ 1989, 752, m.nt. Maeijer, Computerrecht 1989, nr. 2, p. 104, m.nt. Kuitenbrouwer over het recht van betrokkene op inzage en afschrift in het medisch dossier bij de Gemeenschappelijke Medische Dienst van de gemeente Amsterdam. Zie verder Achtergrondstudie ZonMw 2013.
531. Rapport Staatscommissie Grondwet, Den Haag, november 2010, p. 81.
532. Zie Koops, 2011, p.3. Hij betwijfelt of een recht op informationele zelfbeschikking feitelijk bestaat. Volgens hem is onduidelijk wat een subjectief recht op bescherming van persoonsgegevens precies moet behelzen. Wat is de kern van dit grondrecht? Dit wordt niet uitgelegd in het rapport van de Staatscommissie.
533. Zie Hijmans, 2018.
534. Memorie van toelichting UAVG, p.7.
535. Zie Hijmans 2016, paragraaf 4.2, 4.3 en 6.2.
536. Zie advies European Data Protection Supervisor van 7 maart 2012 over het besluitvormingspakket gegevensbescherming. https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.

land artikel 10 Grondwet, inclusief de artikelen 2 en 3, relevant. Vandaar dat deze paragraaf over artikel 10 Grondwet wordt vervolgd.

In de rechtspraak is aangenomen dat artikel 10 Grondwet een algemeen persoonlijkheidsrecht omvat.[537] In het bijzonder is in dit verband de zaak Valkenhorst relevant, die betrekking had op iemand die de identiteit van haar biologische vader wilde achterhalen.[538] Haar moeder wilde deze identiteit niet prijsgeven, maar de gegevens waren ook in bezit van de Stichting Valkenhorst, die de moeder bij de geboorte had opgevangen. De vraag was dan ook of deze stichting op grond van artikel 10 Grondwet kon worden gedwongen de gegevens prijs te geven, of juist de wens van de moeder moest respecteren en de identiteit van de vader geheim moest houden. Advocaat-generaal (A-G) Koopmans beredeneerde dat privacy bij het kennen van de eigen identiteit een belangrijk element is. Volgens de advocaat-generaal valt dit element te lezen in het algemeen persoonlijkheidsrecht, omdat het geacht moet worden aan artikel 10 Grondwet ten grondslag te liggen. De advocaat-generaal beredeneert een en ander aan de hand van een uitspraak van het Duitse *Bundesverfassungsgericht*:

> *"… waarin het recht van het kind op kennis van de eigen afstamming wordt afgeleid uit door het Grundgesetz beschermde waarden, namelijk het recht op vrije ontplooiing van de persoonlijkheid in combinatie met de menselijke waardigheid … Deze beide grondrechten waarborgen ieder individu, aldus het gerecht, 'einen autonomen Bereich privaterLebensgestaltung, in dem er seine individualitätentwicklen und werten kann'."*
> *"… de gedachte van de autonomie van het individu, die aan een groot deel van ons vermogensrecht ten grondslag ligt, steunt op het bestaan van een persoonlijkheidsrecht. … Het kind dat kennis van gegevens omtrent de afstamming eist, oefent derhalve een grondrecht uit."*[539]

De Hoge Raad volgde op dit punt de conclusie van A-G Koopmans. Hierdoor heeft een persoon in de omstandigheden als die van R. jegens een stichting als Valkenhorst aanspraak om op haar verzoek bekend te worden gemaakt met de aan die stichting bekende gegevens omtrent haar ouders'.[540]

Belangrijk is bovendien dat de Hoge Raad in Valkenhorst uitdrukkelijk overwoog dat in het algemeen het recht van een meerderjarig natuurlijk kind om te weten door wie het is verwekt, zwaarder zal wegen dan het recht van de moeder om dit voor haar kind verborgen te houden. Volgens de Hoge Raad houdt dit mede verband met het feit dat het hier gaat om een voor het kind vitaal belang. Bij dit alles noemt de Hoge Raad het zelfbeschikkingsrecht weliswaar niet als basis of leidende notie, maar gelet op de conclusie van de A-G kan deze relatie in de uitspraak toch wel worden gevonden.

Tot nu toe werd artikel 10 Grondwet vooral gezien als een manier om het privéleven van burgers te beschermen tegen de macht van de Staat. In hoofdstuk 2 bleek dat databedrijven ook een grote machtsfactor zijn. Dient de overheid via

537. Zie ook Nehmelmans, 2002.
538. HR 15 april 1994, NJ 1994, 608, m.nt. Hammerstein-Schoonderwoerd.
539. Conclusie A-G Koopmans, punt 18.
540. R.o. 3.2.

de Grondwet burgers ook te beschermen tegen de digitale praktijken van bedrijven, zelfs als die burgers zelf met die bedrijven in zee zijn gegaan?[541] Of kan met een aanvulling op het gegevensbeschermingsrecht worden volstaan?

In het algemeen geldt volgens de Nederlandse wetgever buiten de werkingssfeer van artikel 10, lid 1, Grondwet als algemeen uitgangspunt dat bij de bescherming van persoonsgegevens 'noch de handelingsvrijheid van de degene die persoonsgegevens verwerkt, noch het recht op bescherming van de persoonlijke levenssfeer van de betrokkene in abstracto zwaarder weegt'. Zo blijkt uit de memorie van toelichting bij de Wbp.[542]

> *"In het Nederlandse systeem geldt buiten de werkingssfeer van artikel 10, eerste lid, van de Grondwet als algemeen uitgangspunt dat noch de handelingsvrijheid van de degene die persoonsgegevens verwerkt, noch het recht op bescherming van de persoonlijke levenssfeer van de betrokkene in abstracto zwaarder weegt. Als in een concreet geval beide belangen dreigen te botsen, dienen zij tegen elkaar te worden afgewogen, waarbij rekening moet worden gehouden met de bijzondere (grondwettelijke) waarde van het recht op bescherming van de persoonlijke levenssfeer. Het wetsvoorstel beoogt slechts voor deze afweging het nodige instrumentarium aan te reiken. Het concretiseert in dat verband de criteria aan de hand waarvan moet worden afgewogen, of maakt in een enkel geval, bijvoorbeeld bij gevoelige gegevens, zelf de verlangde afweging."*

Als in een concreet geval bijvoorbeeld de belangen van een verwerkingsverantwoordelijke leverancier van een persoonlijke gezondheidsomgeving dreigen te botsen met belangen van de betrokken persoon als gebruiker, moeten deze belangen tegen elkaar worden afgewogen. Daarbij moet wel rekening worden gehouden met de bijzondere grondwettelijke waarde van het recht op bescherming van de persoonlijke levenssfeer.

6.2.2 Uitvoeringswet AVG

Daar waar de AVG[543] nog ruimte laat voor nationale keuzes, of met het oog op een nadere invulling van regels, heeft de wetgever er uitdrukkelijk voor gekozen om in de Uitvoeringswet voort te bouwen op het huidige normenkader uit Richtlijn 95/46/EG en de Wbp. Enerzijds omdat de tijd ontbrak om op dit moment een geheel nieuw kader te ontwikkelen, anderzijds om de overgang van de oude naar de nieuwe situatie zo soepel mogelijk te laten verlopen.[544] De AVG voorziet op verschillende deelterreinen in nationale beleidsruimte. Een reeks aan bepalingen in de AVG mag of moet worden geïmplementeerd in nationale wetgeving.[545] Zo kunnen lidstaten specifieke regels stellen voor de verwerking van bijzondere gegevens, zoals gezondheidsgegevens. Het is de vraag of de voorge-

541. Dit bepleiten Kool en van Est 2014, explicieter deden zij dat ook in hun opiniestuk dat op 5 februari 2016 verscheen in NRC Handelsblad.
542. MvT Wet bescherming persoonsgegevens, Kamerstukken II, 1997-1998, 25 892, nr. 3, p. 9.
543. Voor Nederlandstalige literatuur over de AVG en de UAVG zie onder andere: Berkvens & Jakimowicz 2016, Holvast 2016, Nouwt 2016, Schermer, Hagenau & Falot, 2017, Versmissen, Terstegge & Krijgsman 2017, Von Meijenfeldt 2017, De Zeeuw, 2017, Verhelst 2017, Heijna 2017, Comijs 2017a en 2017b, Lousberg & Cuijpers 2017, Van Balen & Nijveld 2017, Bastiaans 2018, Hijmans, 2018, Van de Bunt & Strijbos, 2018, Hooghiemstra & Nouwt 2018b.
544. Memorie van toelichting UAVG, p. 3.
545. Hijmans, 2018.

stelde UAVG en de AVG steeds met elkaar in overeenstemming zijn. Bijvoorbeeld de regeling in de voorgestelde UAVG van de geautomatiseerde individuele besluitvorming.[546] De UAVG schept een uitzondering op het recht van individuen om niet onderworpen te worden aan automatische besluitvorming[547]. De uitzondering in de UAVG is generiek, maar geldt niet als de besluitvorming plaatsvindt op grond van profilering. De betreffende bepaling in de UAVG is niet noodzakelijkerwijs in lijn met de tekstuele uitleg van artikel 22 AVG en evenmin met de uitleg die de gezamenlijke privacytoezichthouders hebben gegeven.[548] Dit doet de vraag rijzen of artikel 40 van de voorgestelde UAVG in overeenstemming is met de AVG. Het gaat immers om een uitzondering op een door de EU gegarandeerd recht. Zo'n uitzondering dient in de regel beperkt te worden geïnterpreteerd. Bovendien is het voorgestelde artikel 40 gebaseerd op een eigen uitleg van de regering die niet overeenstemt met de uitleg van de Europese toezichthouders.[549]

Voor het onderwerp van deze dissertatie is verder van belang dat de AVG en de UAVG het verwerken van bijzondere persoonsgegevens[550] verbieden.[551] Artikel 30 UAVG behandelt de uitzonderingen op het verbod om gezondheidsgegevens te mogen verwerken. Artikel 30 UAVG is vergelijkbaar met destijds artikel 21 Wbp. Voor hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening geldt in de UAVG dat deze ontheffing hebben van het verwerkingsverbod voor zover de verwerking van gezondheidsgegevens noodzakelijk is voor een goede behandeling of verzorging van de betrokkene of voor het beheer van de betreffende instelling of beroepspraktijk.
Als het noodzakelijk is in aanvulling op de verwerking van gezondheidsgegevens, mogen hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening ook andere bijzondere persoonsgegevens verwerken, zoals gegevens over iemands ras of godsdienst. Maar ook dan moet dat wel noodzakelijk zijn voor een goede behandeling of verzorging van de betrokkene. Zo wordt aangenomen dat een ziekenhuis foto's van patiënten mag vastleggen met het oog op de identificatie van patiënten. Dit om te waarborgen dat de juiste gegevens aan de juiste patiënt worden gekoppeld en om identiteitsfraude te voorkomen.[552]

Verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen mogen met de uitdrukkelijke toestemming van de betrokken persoon (gebruiker) gezondheids- en andere gegevens van de persoon verwerken.

546. Art. 22 AVG en art. 40 voorstel UAVG.
547. Zie over geautomatiseerde besluitvorming – in het bijzonder geautomatiseerde ketenbesluiten – Van Eck (2018) en Widlak & Peeters (2018).
548. Artikel 29 Werkgroep, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', wp251, https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
549. Hijmans, 2018.
550. Comijs, 2017.
551. Artikel 8 en 10 AVG en artikel 22 t/m 31 Uitvoeringswet AVG.
552. CBP d.d. 20 november 2006, kenmerk z2006-01388, advies inzake aanvulling Besluit gebruik burgerservicenummer in de zorg.

Wie persoonsgegevens in het algemeen verwerkt, moet dat kunnen baseren op ten minste één van de grondslagen in artikel 6 AVG. Dat geldt ook voor gezondheidsgegevens.

Een mogelijke grondslag kan zijn dat het verzamelen, vastleggen en verder gebruiken van persoonsgegevens over iemands gezondheid noodzakelijk is ter uitvoering van een overeenkomst tot geneeskundige behandeling of dat dit voortvloeit uit de wettelijke dossierplicht.
Ook de 'ondubbelzinnig toestemming' van de betrokkene is een mogelijke grondslag voor het verzamelen en vastleggen van persoonsgegevens. Wanneer een beroep op andere grondslagen kan worden gedaan, is de toestemming van de betrokkene echter niet nodig.

Voor wat betreft de rechtsbescherming geldt op basis van de UAVG net als nu bij de Wbp een gedifferentieerd systeem van rechterlijke toetsing. Zowel de bestuursrechter als de burgerlijke rechter hebben een taak.

In de AVG en de UAVG heeft de AP naast een corrigerende bevoegdheid ook een uitgebreidere onderzoeksbevoegdheid. Zo kan zij een bevel geven tot het verstrekken van relevante informatie en kan zij ook bedrijfsruimten betreden (zoals de Autoriteit Consument en Markt of Autoriteit Financiële Markten) om informatie te halen en bijvoorbeeld certificeringen te controleren. Daarnaast krijgt de AP diverse autorisatie- en adviesbevoegdheden, bijvoorbeeld in het kader van een dataprotection privacy impact assessment (DPIA), certificeringen, standaardbepalingen, goedkeuringen en toestemmingen.

Voor verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen geldt op grond van de (U)AVG geen wettelijke zwijgplicht, zoals medische hulpverleners die hebben in de zin van de Wet BIG en de WGBO. Ook hebben zowel de verwerkingsverantwoordelijken van persoonlijke gezondheidsgegevens als de betrokken personen geen verschoningsrecht in de zin van artikel 218 Sv.

De hierna volgende gezondheidsrechtelijke wetgeving betreft informationele zelfbeschikkingsrechten die specifiek in de Nederlandse zorgcontext van toepassing zijn.

6.2.3 Wet op de geneeskundige behandelingsovereenkomst

In subparagraaf 6.2.1 kwam aan de orde dat artikel 11 Grondwet eveneens betrekking heeft op de relatie tussen hulpverlener en patiënt en daarmee ten grondslag ligt aan de wettelijke regeling van de geneeskundige behandelingsovereenkomst (WGBO), boek 7, artikel 7:446 e.v. BW. Naast lichamelijke zelfbeschikkingsrechten bevat de WGBO ook zelfbeschikkingsrechten met betrekking tot medische dossiers.[553] Het gaat om de navolgende zeven zelfbeschikkingsrechten.

553. Zie hierover bijvoorbeeld ook Hustinx 1999, en Ploem, 1999, pp. 301-305.

1. Recht op niet-weten
De patiënt heeft het recht om geen inlichtingen te willen ontvangen.[554] De wetgever heeft daarmee het zelfbeschikkingsrecht om geen informatie te hoeven ontvangen, erkend. Op dit recht op niet-weten heeft de wetgever echter wel een beperking aangebracht. Als de hulpverlener van mening is dat het niet-weten voor de patiënt zelf of voor een ander nadelig is of kan zijn, en het belang van de patiënt bij niet-weten daar niet tegenop weegt, dan dient de hulpverlener de informatie toch te verstrekken aan de patiënt.[555]

2. Dossierplicht
De WGBO bevat een dossierplicht voor hulpverleners.[556] Hulpverleners zijn op grond hiervan verplicht om een dossier in te richten met betrekking tot de behandeling van de patiënt. In dat dossier moet de hulpverlener aantekeningen bijhouden van de gegevens over de gezondheid van de patiënt en van de verrichtingen die bij de patiënt zijn uitgevoerd. Ook andere stukken die zodanige gegevens bevatten, moeten in het dossier worden opgenomen. Alleen aantekeningen die noodzakelijk zijn voor een goede hulpverlening aan de patiënt mogen in het dossier worden opgeslagen. De hulpverlener heeft geen exclusieve eigendomsrechten op het medisch dossier, maar wel verantwoordelijkheden en zekere zelfbeschikkingsrechten, net als patiënten die hebben.[557]

3. Bewaartermijn
Een hulpverlener is verplicht om de 'bescheiden' – dat wil zeggen aantekeningen van gegevens over de gezondheid van de patiënt en andere stukken die gezondheidsgegevens bevatten – ten minste vijftien jaar te bewaren[558], of zo veel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit.[559] Langer dan vijftien jaar bewaren is nodig als de gegevens voor een goede hulpverlening aan de patiënt beschikbaar moeten blijven. Dat zou bijvoorbeeld kunnen gelden voor patiënten met een chronische ziekte. Langer bewaren van gegevens is altijd aan de orde bij genetisch onderzoek voor eventueel toekomstig advies aan familieleden. Als een patiënt binnen die vijftien jaar gebruikmaakt van zijn vernietigingsrecht[560] dan moet daaraan tegemoet worden gekomen en blijven de gegevens dus niet vijftien jaar lang bewaard. De bewaartermijn begint te lopen op het moment dat de behandeling is geëindigd.

554. Recht op niet-weten: artikel 7:449 BW.
555. Zie L.F. Markenstein, Tekst en toelichting WGBO. Editie 2006. Den Haag: Sdu Uitgevers 2005, p. 36; J.M.Witmer, R.P. de Roode (eindred.), Van wet naar praktijk. Implementatie van de WGBO. Deel 2. Informatie en toestemming. Utrecht, 2004.
556. Artikel 7:454 BW.
557. Zie Hooghiemstra en Ippel 2011, p.7.
558. Gezondheidsraad 2004. In dit advies over de bewaartermijn voor patiëntengegevens werd een wetswijziging bepleit van de oude bepaling in de WGBO die uitging van een bewaartermijn van 10 jaren. De Gezondheidsraad heeft overigens geen vijftien jaar geadviseerd, maar een bevriezing van 5 jaar na het uitkomen van het advies om nader te onderzoeken wat gewenste bewaartermijnen zouden zijn voor bijzondere situaties, zoals bij erfelijkheidsgegevens en medisch wetenschappelijk onderzoek.
559. Artikel 7:454 lid 3 BW.
560. Zie hierna: artikel 7:455 BW.

4. Recht op vernietiging
Het meest vergaande zelfbeschikkingsrecht van patiënten is het recht om te verzoeken om vernietiging van het medisch dossier.[561] Als een patiënt daarom verzoekt, is een hulpverlener verplicht om de inhoud van het medisch dossier binnen drie maanden te vernietigen. Die vernietigingsplicht geldt echter niet als het om informatie gaat die belangrijk is voor een ander dan de patiënt. Informatie over erfelijke ziekten kan bijvoorbeeld mede van belang zijn voor familieleden van de patiënt.
Opvallend is dat een hulpverlener een verzoek om vernietiging van onderdelen uit een medisch dossier niet mag weigeren op grond van een belang van de patiënt zelf.

5. Recht op inzage en afschrift
Een ander zelfbeschikkingsrecht van de patiënt is het recht op inzage en afschrift.[562] Behoudens als dat noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander, mag een hulpverlener een verzoek van een patiënt om inzage in of afschrift van het medisch dossier niet weigeren. Een hulpverlener mag een patiënt de inzage ook niet onthouden wegens het risico van mogelijke schade bij kennisneming van bepaalde informatie. Op grond van artikel 12.5 AVG dient een afschrift kosteloos te zijn.

6. Blokkeringsrecht
Het blokkeringsrecht[563] is het recht dat degene die een keuring ondergaat, heeft om na kennis te hebben genomen van de uitslag van de keuring en de gevolgtrekking die daaraan wordt verbonden, de doorgifte daarvan aan de opdrachtgever (werknemer, verzekeraar of opleiding), tegen te houden.[564]

7. Medisch beroepsgeheim: recht en plicht
Het medisch beroepsgeheim is een beproefde traditionele notie. In de eed van Hippocrates is de eerste omschrijving van het beroepsgeheim te vinden. Er is al een befaamd arrest van de Hoge Raad uit het begin van de vorige eeuw over het medisch beroepsgeheim[565], waarin wordt gesteld *'vermits alleen bij voldoening aan dien eisch (*van geheimhouding) *kan wordenvoorkomen dat de zieken zelve (…) uit vrees voor zijn openbaarheid zich latenweerhouden geneeskundige hulp in te roepen'.*

Het schenden van geheimhoudingsregels is strafbaar op grond van art. 272 Sr, dat straf stelt op diegene, die een geheim, waarvan hij weet of redelijkerwijs moet vermoeden, dat hij dat uit hoofde van zijn beroep verplicht is te bewaren, opzettelijk schendt. De patiënt kan de arts ook op grond van artikel 47 Wet BIG een tuchtrechtelijk verwijt maken, hetgeen gevolgen kan hebben voor de beroepsuitoefening van de arts, bijvoorbeeld als de uitspraak van het tuchtcollege een schorsing of ontzegging het beroep van arts uit te oefenen inhoudt.

561. Artikel 7:455 BW.
562. Artikel 7:456 BW.
563. Artikel 7:464 BW.
564. Markenstein, 2006, p. 72 e.v.
565. HR 21 april 1913, NJ 1913, 959.

Daarnaast kan een patiënt de arts en het ziekenhuis civielrechtelijk aansprakelijk stellen, indien hij meent dat het medisch beroepsgeheim is geschonden. In het navolgende komt het medisch beroepsgeheim uit de WGBO aan de orde en aan het einde van dit onderdeel nog enkele reflecties op het verschoningsrecht, als onderdeel van het medisch beroepsgeheim, zoals geregeld in artikel 218 Sv.

In hoofdstuk 3[566] kwam aan de orde dat het medisch beroepsgeheim bestaat uit de zwijgplicht en het verschoningsrecht voor hulpverleners. De keerzijde van de zwijgplicht voor hulpverleners is een recht van patiënten op geheimhouding van hun gegevens.[567] Een hulpverlener mag niet zonder toestemming van de patiënt informatie uit het medisch dossier aan anderen verstrekken. Dat is de hoofdregel.
Met uitdrukkelijke toestemming van de patiënt mag een hulpverlener gegevens aan derden verstrekken. De toestemming verplicht de hulpverlener niet om te spreken. De hulpverlener dient immers ook het individuele en collectieve belang van het beroepsgeheim mee te wegen.

Het medisch beroepsgeheim dient een algemeen en een individueel belang. Het algemeen belang bestaat uit het waarborgen van de vrije toegang tot verlening van hulp en bijstand op het gebied van de gezondheidszorg. Dit algemeen belang is met name een zelfstandig toetspunt bij de vraag of er verschoningsrecht bestaat voor de beroepsbeoefenaar in de individuele gezondheidszorg. Met andere woorden: het 'maatschappelijk belang dat een ieder zich vrijelijk en zonder vrees voor openbaarmaking van het toevertrouwde om bijstand en advies tot de verschoningsgerechtigde c.q. zwijgplichtige moet kunnen wenden'.[568]

In het verlengde van het algemene belang dient het medisch beroepsgeheim ook het individuele belang van de patiënt. Een patiënt moet erop kunnen vertrouwen dat de informatie die hij aan de hulpverlener verschaft niet zonder zijn toestemming of zonder dat de wet dat toestaat voor andere doeleinden wordt gebruikt of aan anderen wordt verstrekt. Het individuele belang bestaat uit een privacybelang (vertrouwen dat de meest intieme informatie niet bij anderen terecht komt) en een individueel gezondheidsbelang (vrij zijn om de meest intieme informatie te verstrekken teneinde zo goed mogelijk behandeld te kunnen worden). Het belang van het medisch beroepsgeheim is daarmee niet alleen het belang om 'iets te verbergen', maar bestaat ook uit achterliggende gezondheidsbelangen.

Op twee plaatsen in de wet is een beroepsspecifieke zwijgplicht opgenomen voor medische hulpverleners. In de eerste plaats is dat artikel 88 van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). Dit artikel bepaalt dat een ieder die een beroep op het gebied van de individuele gezondheidszorg

566. Zie paragraaf 3.4.
567. Artikel 7:457 BW.
568. Dit belang is door de Hoge Raad herhaalde malen erkend, o.a. HR 19 november 1985, NJ 1986, 533, met annotatie van 't Hart (Verschoningsrecht).

uitoefent, de plicht heeft alles geheim te houden wat hem bij de uitoefening van zijn beroep is toevertrouwd. Daarnaast is de medische zwijgplicht vastgelegd in artikel 7:457 BW.

Op de hoofdregel dat een hulpverlener niet zonder toestemming van de patiënt informatie uit het medisch dossier aan anderen mag verstrekken, bestaan enkele uitzonderingen. Zo is de toestemming niet nodig als een wet tot verstrekking van de gegevens verplicht.[569]
Voorbeelden van wettelijke verplichtingen om patiëntgegevens te verstrekken zijn te vinden in de Wet publieke gezondheid (infectieziekten) en in de Wet op de lijkbezorging (melding van natuurlijk overlijden). Ook is toestemming niet nodig als het noodzakelijk is om informatie uit het dossier te verstrekken aan degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst of aan degene die optreedt als vervanger van de hulpverlener.[570]

Ook voor de verstrekking van informatie aan een vertegenwoordiger van de patiënt die instemming moet verlenen aan de uitvoering van de behandelingsovereenkomst, is uiteraard geen toestemming nodig van de patiënt zelf.[571]
Verder mogen patiëntgegevens aan een derde partij worden verstrekt als sprake is van een conflict van plichten. Dit doet zich voor als de hulpverlener ernstige schade voor de patiënt of een ander kan voorkomen door het beroepsgeheim te doorbreken. Een andere situatie is dat sprake is van 'zwaarwegende belangen' of van 'zeer uitzonderlijke omstandigheden' op grond waarvan bijvoorbeeld het OM patiëntendossiers bij hulpverleners in beslag mag nemen.[572] Ook wanneer tegen een zorgverlener een klacht is ingediend, bijvoorbeeld bij een klachtencommissie of tuchtcollege, moet de zorgverlener patiëntgegevens kunnen overleggen als dat nodig is om zich te verweren tegen die klacht. Bovendien gelden bijzondere voorwaarden op grond waarvan zonder toestemming van de patiënt gegevens mogen worden verstrekt voor wetenschappelijk onderzoek of statistiek.

Wat betreft de context van politie en justitie komt er met het wetsvoorstel tot vaststelling van Boek 1 van het nieuwe Wetboek van Strafvordering mogelijk op termijn duidelijkheid ten gunste van een verschoningsrecht, zoals op dit moment vastgelegd in artikel 218 Sv. De planning is dat de boeken 1-6 nieuw Wetboek van Strafvordering in januari 2019 aan de Raad van State worden voorgelegd en in de loop van 2019 bij de Tweede Kamer worden ingediend. Op dit moment worden de adviezen over deze boeken in de voorstellen verwerkt.[573] In het wetsvoorstel tot vaststelling van Boek 1 van het nieuwe Wetboek van Strafvordering wordt met verwijzing naar de uitspraak van de Hoge Raad in 1985 voorgesteld om uitdrukkelijker in de wet op te nemen dat het verschoningsrecht zich niet

569. Artikel 7:457 lid 1 BW.
570. Artikel 7:457 lid 2 BW.
571. Artikel 7:457 lid 3 BW.
572. KNMG Handreiking Beroepsgeheim en politie/justitie, p. 33.
573. Zie de voortgangsbrief aan de Kamer van 20 december 2017: https://www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering/documenten/kamerstukken/2017/12/20/tk-aanpassing-planning-wetgevingsprogramma-modernisering-van-het-wetboek-van-strafvordering.

alleen uitstrekt over informatie die de betrokkene aan de verschoningsgerechtigde toevertrouwt, maar ook over informatie die de verschoningsgerechtigde binnen de vertrouwensrelatie aan de betrokkene verstrekt en over eventuele waarnemingen die binnen de vertrouwensrelatie hebben plaatsgevonden. Daarom wordt voorgesteld de zinsnede uit het huidige artikel 218 Sv 'Waarvan de wetenschap aan hen als zoodanig is toevertrouwd' te vervangen door 'omtrent de wetenschap over hetgeen rechtstreeks verband houden met de verschoningsgerechtigde werkzaamheden'. Daarmee wordt tot uitdrukking gebracht dat het moet gaan om een daadwerkelijk verband en niet om een ver verwijderd, zijdeling verband.

Artikel 218 Sv verwijst naar degene die uit hoofde van stand, ambt of beroep tot geheimhouding verplicht is, en dan naar de informatie die hij 'als zodanig' (dus in het kader van stand, ambt of beroep) verkregen heeft. Het is een recht waarop (medische) beroepsbeoefenaren zich kunnen beroepen als zij anderszins al een geheimhouding hebben.
Kijkend naar de beoogde wijziging van artikel 218 Sv, kan een leverancier van een gezondheidsomgeving zich nu niet beroepen op een verschoningsrecht ter zake van de gegevens die daarin staan, omdat hij die informatie niet onder zich heeft uit hoofde van stand, ambt of beroep en er uit dien hoofde ook geen geheimhoudingsplicht geldt. Het lijkt mij dat de beoogde verbreding van artikel 218 Sv dat niet anders maakt, want de informatie van degene die zich op verschoning beroept wordt wel verruimd, maar niet de kring van personen (laat staan rechtspersonen) die zich erop kan beroepen bij de rechter.

Om het eerder genoemde 'patiëntgeheim' voor gegevens in gezondheidsomgevingen net zo te regelen als het medisch beroepsgeheim, zal er een wettelijke zwijgplicht (geheimhoudingsplicht) voor de leverancier moeten komen en een verschoningsrecht. Het verschoningsrecht zou nog bij de herziening van artikel 218 Sv expliciet meegenomen kunnen worden. Daarbij is een omschrijving noodzakelijk die breder is dan stand, ambt en beroep, en moet dus ook nog geregeld worden dat het niet alleen natuurlijke, maar ook rechtspersonen zijn die zich erop kunnen beroepen, als dat mogelijk is.

Uit het voorgaande blijkt dat een persoonlijke gezondheidsomgeving ten minste ten dele niet onder het medisch beroepsgeheim valt. Daarom lijkt een wettelijk recht voor personen op geheimhouding van hun gegevens – wel aangeduid als 'patiëntgeheim' – noodzakelijk om te voorkomen dat gezondheidsgegevens min of meer vogelvrij worden. Het ligt voor de hand om dit vorm te geven naar het voorbeeld van het medische beroepsgeheim, dus in de vorm van een zwijgplicht van de leverancier van een persoonlijke gezondheidsomgeving en een verschoningsrecht voor de betreffende persoon en de leverancier van diens persoonlijke gezondheidsomgeving. De Wet BIG en de WGBO bevatten geen zwijgplicht voor het verwerken van gezondheidsgegevens door verwerkingsverantwoordelijken die geen medische hulpverleners zijn. Voor verwerkingsverantwoordelijken en betrokkenen die gezondheidsgegevens buiten de geneeskundige behandelrelatie verwerken zijn plichten en rechten noodzakelijk in aanvulling op de AVG, zonder ze te vermengen met de bijzon-

dere context van de geneeskundige behandelrelatie met het bijbehorende medisch beroepsgeheim.

Tot slot blijft het debat actueel over het medisch beroepsgeheim door allerhande nieuwe bevoegdheden van derden,[574] zoals bij het debat over de Wet inlichtingen- en Veiligheidsdiensten (Wiv).[575] Deze ontwikkeling betekent dat informationele zelfbeschikking in de zorg daarmee ook onder druk staat. Aan de ene kant is zichtbaar dat er steeds actievere informationele zelfbeschikkingsrechten bij komen in de zorg, terwijl aan de andere kant de uitholling van het medisch beroepsgeheim, onder andere door nieuwe bevoegdheden van derden, in specifieke situaties de informationele zelfbeschikkingsrechten aantasten.

Op 6 november 2017 bracht de procureur-generaal bij de Hoge Raad der Nederlanden het rapport 'Gedeelde informatie' uit.[576] De PG deed in het kader van het in art. 122, lid 1, Wet Rechterlijke Organisatie (Wet RO) bedoelde toezicht onderzoek naar de vraag of voor het toevoegen door het OM van – kort gezegd – strafrechtelijke gegevens aan het dossier Bijzondere opnemingen psychiatrische ziekenhuizen (BOPZ) het thans geldende wettelijke kader een grondslag kan worden gevonden en of het toevoegen van strafrechtelijke gegevens aan het BOPZ-dossier, vooruitlopend op de op stapel staande wetgeving met betrekking tot gedwongen zorg, rechtmatig is. De belangrijkste bevinding van het rapport is dat naar aanleiding van de aanbevelingen van de Commissie Hoekstra het OM feitelijk is begonnen met het voegen van strafrechtelijke gegevens in het BOPZ-dossier, zonder voldoende duidelijk vast te stellen of het hiertoe op grond van de actuele gegevensbeschermingswetgeving wel in alle gevallen bevoegd is en zonder zich voldoende rekenschap te geven van de voorwaarden die hierbij in acht moeten worden genomen.

De aanleiding voor het rapport van de procureur-generaal bij de Hoge Raad der Nederlanden voert terug op de gewelddadige dood van Els Borst, voormalig minister van volksgezondheid. De Commissie Hoekstra heeft een onderzoek ingesteld naar eventuele structurele tekortkomingen in werkprocessen van het OM en andere instanties aangaande, kort gezegd, 'verwarde personen'. Sinds 2016 is het OM naar aanleiding van de aanbevelingen van de Commissie Hoekstra begonnen met het structureel inbrengen van strafrechtelijke gegevens bij verzoeken tot een dwangopname op grond van de Wet BOPZ. Het doel hiervan is

574. Zoals het debat en het referendum over de Wet inlichtingen- en veiligheidsdiensten(Wiv) 2017 en het debat over de wijziging van de Wet marktordening gezondheidszorg en enkele andere wetten in verband met het verbeteren van toezicht, opsporing, naleving en handhaving. Deze wetswijziging voorziet (slechts) in een uitbreiding van een reeds bestaande wettelijke grondslag voor materiële controle. Deze grondslag bestaat al voor de naturapolis en voor de restitutiepolis, maar bevat een lacune voor de situatie dat de zorgaanbieder en verzekeraar geen contract hebben. Dat wordt met de wijziging gelijk getrokken voor alle polissen.
575. Overigens is de KNMG tevreden met de toezeggingen van de AIVD na kritische vragen van de KNMG over de Wiv, zie https://www.icthealth.nl/nieuws/knmg-tevreden-over-toezeggingen-aivd-bij-gebruik-sleepwet/.
576. Spronken & Koopmans, 2017.

dat de rechter zich met behulp van deze informatie een beter beeld kan vormen over de noodzaak van een (voortgezette) dwangopname.[577]

Naast de WGBO zijn de zelfbeschikkingsrechten, neergelegd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz), van belang.

6.2.4 Wabvpz

Op 1 juli 2017 is de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) in werking getreden. Deze wet is een aanvulling op onder andere de AVG, de WGBO, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet.

Op 5 april 2011 verwierp de Eerste Kamer het wetsvoorstel over het landelijk Elektronisch Patiënten Dossier (EPD)[578]. Daarbij werd een motie aangenomen (motie Tan) waarin de regering werd verzocht om te komen tot een nadere wettelijke regeling van de digitale dossiervorming en overdracht van gegevens. Met de Wabvpz en het bijbehorende Besluit elektronische gegevensverwerking door zorgaanbieders is invulling gegeven aan dit verzoek.[579] Overigens beperkt de reikwijdte van Wabvpz zich tot elektronische uitwisselingssystemen in de zorg. Onder een 'elektronisch uitwisselingssysteem' wordt op grond van artikel 1, onderdeel j van deze wet verstaan:

> *"een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, waaronder niet begrepen een systeem binnen een zorgaanbieder, voor het bijhouden van een elektronisch dossier."*

Tijdens de behandeling van deze wet in de Eerste Kamer is onder andere de motie-Bredenoord (D66) c.s. aangenomen over de verdere uitwerking van *dataprotectie-by-design* als het uitgangspunt voor de elektronische verwerking van medische gegevens.[580] In het volgende hoofdstuk, in subparagraaf 7.2.1 over *privacy-by-design*, komt deze motie nader aan de orde.

577. Zie NJB 2017/2132 Delen van gegevens door het OM in het kader van een BOPZ machtiging Procureur-generaal constateert tekortkomingen Datum 06-11-2017.
578. Beter was destijds de ook toen al bestaande term Landelijk Schakel Punt (LSP), zie 6.3.5., te hanteren, omdat met het Landelijk EPD ten onrechte het beeld ontstond dat op landelijk niveau alle elektronische dossiers van patiënten zouden worden verzameld, terwijl het feitelijk om een verwijsindex gaat die aan de hand van het BSN en een zorgaanbiedernummer het waarneemdossier huisartsen- en het medicatiedossier verwerkt dat onder de verwerkingsverantwoordelijkheid blijft van de betreffende huisartsen en apothekers.
579. Als directeur van de Raad voor Volksgezondheid en Samenleving (RVS) en expert mocht ik tijdens de deskundigenbijeenkomst van de Eerste Kamer en het Rathenau Instituut op 13 april 2015 mijn reflectie geven bij dit wetsvoorstel. Voor het verslag zie: Eerste Kamer der Staten-Generaal, Vergaderjaar 2014–2015, 33 509, Wijziging van de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens), Verslag van gesprek met deskundigen, vastgesteld 26 mei 2015.
580. EK 33.509, R.

Op grond van deze wet kan de cliënt drie jaar na de inwerkingtreding zijn medisch dossier zelf elektronisch inzien. De reden dat de minister van VWS ervoor heeft gekozen om bij elektronische inzage van medische dossiers een overgangsperiode van drie jaar toe te kennen, is het feit dat in de gezondheidszorg – en overigens ook elders in Nederland – nog geen breed beschikbare authenticatiemiddelen op een hoog betrouwbaarheidsniveau beschikbaar zijn.[581] Uit onderzoek[582] in opdracht van de minister van VWS bleek dat in veel gevallen dit hoge betrouwbaarheidsniveau noodzakelijk is.

Wat toestemming betreft bevat deze wet de bepaling dat voor beschikbaarstelling van gegevens via een elektronisch uitwisselingssysteem de zorgaanbieder de voorafgaande toestemming van de betreffende cliënt behoeft.[583] Hij dient voorts een registratie bij te houden van de door cliënten verleende toestemming waarbij wordt aangetekend vanaf welk moment de toestemming van kracht is geworden. Bij dit alles gaat het om zogenoemde 'gespecificeerde toestemming', dat wil zeggen toestemming voor het beschikbaar stellen van alle of bepaalde gegevens aan bepaalde door de cliënt aan te duiden specifieke zorgaanbieders of categorieën van zorgaanbieders.[584] In deze benadering zijn alle categorieën van zorgaanbieders die de persoon niet expliciet heeft benoemd automatisch uitgesloten van het raadplegen van zijn gegevens, die beschikbaar zijn gesteld in een elektronisch uitwisselingssysteem.

Het Besluit elektronische gegevensverwerking door zorgaanbieders is per 1 januari 2018 in werking getreden en als besluit 'onder' de Wabvpz gehangen. In dit besluit zijn specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling door zorgaanbieders vastgelegd. De eisen zijn in een besluit neergelegd in plaats van in een wet, om eenvoudiger te kunnen inspelen op de actuele stand van de techniek.

Dit besluit gaat onder andere over het gebruik van het burgerservicenummer (BSN) in de zorg en is van toepassing op alle zorgaanbieders die zijn aangesloten op uitwisselingssystemen in de zorg. In de praktijk zijn bijna alle huisartsen, apothekers en ziekenhuizen in de Nederlandse zorg aangesloten op een uitwisselingssysteem, waarmee dit besluit de facto voor vrijwel alle zorgaanbieders geldt. Op grond van dit besluit is de laatste uitgave van de in het besluit genoemde NEN-normen van toepassing. Overigens werd die plicht in juni 2009 al gekoppeld aan het gebruik van het BSN in de zorg. Bij de NEN-norm voor informatiebeveiliging, NEN 7510, gaat het op dit moment om de NEN 7510:2017.

In het besluit staat verder onder andere de verplichting om een Functionaris Gegevensbescherming (FG) te benoemen als door zorginstellingen op grote

581. Diverse private middelen leveranciers stellen op dit moment authenticatiemiddelen op niveau hoog (eIDAS) te kunnen leveren. Op kleine schaal worden die middelen ook al gebruikt, onder andere in pilots. Om ze voor alle personen in Nederland breed beschikbaar te krijgen is echter financiering noodzakelijk. Ook zal de claim dat deze middelen aan niveau hoog voldoen onafhankelijk moeten worden geverifieerd.
582. PrivacyCare & PBLQ 2016.
583. Artikel 15a, lid 1, Wet aanvullende bepalingen verwerking persoonsgegevens.
584. Artikel 15a, lid 2, Wet aanvullende bepalingen verwerking persoonsgegevens.

schaalpersoonsgegevens worden verwerkt. Onduidelijk is hoe deze bepaling zich verhoudt tot de bepalingen in de AVG over de FG[585]. De AVG heeft in ieder geval een bredere reikwijdte, want heeft in beginsel betrekking op alle verwerkingsverantwoordelijken en verwerkers[586]. Verder kan worden vastgesteld dat al sinds 1 januari 2018 verwerkingsverantwoordelijken voor een elektronisch uitwisselingssysteem, zoals bedoeld in de Wabvpz en voor zorginstellingen als bedoeld in artikel 1 lid 1 Wet kwaliteit, klachten en geschillen zorg (Wkkgz) die op grote schaal bijzondere gegevens verwerken verplicht waren een FG te benoemen.[587]

Op grond van de AVG is de AP toezichthouder voor de Wabvpz en de bijbehorende Algemene maatregel van bestuur (AMvB). De Inspectie Gezondheidszorg & Jeugd (IGJ) heeft op grond van de Kwaliteitswet zorginstellingen tot taak toezicht te houden op verantwoorde zorg en zal de onderdelen van NEN-normen die hiervoor relevant zijn, in haar toezicht betrekken. De IGJ en de AP hebben een samenwerkingsprotocol waarin de afspraken tussen de AP en de IGJ over de wijze van samenwerking bij het toezicht staan opgesteld.

6.2.5 NEN 7510: 2017

Specifiek voor informatiebeveiliging in de zorg is de nieuwe NEN 7510 van 2017 (en NEN 7512 en 7513) relevant. De IGJ en de AP hanteren bij hun onderzoeken en audits inzake informatiebeveiliging in de zorg deze norm(en). De normen geven concreet houvast aan de abstracte normen uit de AVG en zijn bovendien een concrete Nederlandse invulling van de meer wereldwijde ISO-normen en Europese CEN-normen.
De nieuwe norm biedt een integraal kader voor informatiebeveiliging, toegespitst op de Nederlandse situatie. Opvallend in de NEN 7510:2017 is dat de reikwijdte van deze geactualiseerde norm zich niet beperkt tot de gegevens bij zorgaanbieders, maar zich ook uitstrekt tot het verwerken van gezondheidsgegevens buiten de zorg, zoals bij persoonlijke gezondheidsomgevingen.

> Ter illustratie staat in de NEN 7510: 2017 de volgende beheersmaatregel:
> – Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
> Met als zorgspecifieke beheersmaatregel:
> – *De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken*, behoort onderhevig te zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers behoren te garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken.
> – De gebruikersregistratiegegevens behoren regelmatig te worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.

585. Zie De Zeeuw, 2017.
586. Verwerkers zijn in artikel 4 lid 8 AVG wat in de Wbp bewerkers waren: 'Een natuurlijke persoon of rechtspersoon, een overheidsinstantie. Een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt'.
587. Aldus artikel 2 Besluit elektronische gegevensverwerking door zorgaanbieders (Stb. 2017, 446).

In de ter illustratie getoonde beheersmaatregelen van de NEN 7510:2017 is '*De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken*' gecursiveerd, omdat hieruit blijkt dat deze norm zich niet meer alleen beperkt tot zorgaanbieders, maar van toepassing is op alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, dus ook op persoonlijke gezondheidsomgevingen. Daardoor is de NEN 7510:2017 voor deze dissertatie relevant.[588] Artikel 42 AVG roept op tot bevordering van certificeringsmechanismen. De NEN 7510:2017 is voor persoonlijke gezondheidsomgevingen te hanteren als certificeringsmechanisme.[589]

6.3 RECHTSPRAAK

Uit de Nederlandse rechtspraak blijkt in hoeverre in de praktijk informationele zelfbeschikking aan de orde is. In subparagraaf 6.2.1 kwam het Valkenhorst-arrest uit 1994[590] al aan de orde. Naast de rechterlijke uitspraken worden een aantal relevante beslissingen van Tuchtcolleges, de AP en de IGJ behandeld.

6.3.1 Santander

De zaak Santander gaat over een man die een schuld had bij Santander. Het lukt Santander niet om het periodieke bedrag van € 20 te incasseren. Daarop heeft Santander de man aangeschreven om het resterende bedrag van € 315,18 op te eisen. Ook is de man meegedeeld dat bij drie termijnen betalingsachterstand er een registratie bij het Bureau Kredietregistratie (BKR) zou volgen. In latere brieven is de man nog enkele keren gesommeerd het bedrag te betalen. Deze brieven hebben de man vanwege een verhuizing nooit bereikt. Toen betaling uitbleef, heeft Santander de man geregistreerd bij het BKR.
Santander heeft uiteindelijk de vordering overgedragen aan een deurwaarder die de man op zijn nieuwe adres weet te vinden. De man betaalt zijn schuld aan Santander. De registratie bij het BKR blijft echter, waardoor de man geen hypothecaire lening bij een bank kan krijgen. De man beroept zich op de Wbp. Santander weigert de registratie bij het BKR op te heffen. Volgens Santander is de melding bij het BKR gerechtvaardigd vanwege het feit dat zij niets meer heeft gedaan dan een betalingsachterstand op een krediet en de maximale hoogte van dat krediet te melden bij het BKR.
Daarop start de man een procedure bij de rechtbank om de gegevens alsnog uit het BKR-register verwijderd te krijgen. De rechtbank heeft dit verzoek toegewezen. Daarop gaat Santander in hoger beroep. Dat hoger beroep wordt door Santander verloren. Het gerechtshof bekrachtigt de beschikking van de rechtbank. Santander gaat daarop in cassatie bij de Hoge Raad. Ook het beroep in cassatie wordt door Santander verloren. De Hoge Raad heeft in zijn beschikking van 9 september 2011[591] benadrukt dat voor verwerking van persoonsgegevens altijd een grondslag in de zin van artikel 8 Wbp aanwezig moet zijn. Daarbij wijst de

588. Zie ook paragraaf 7.2.2.
589. Zie over het gebruik van technische normen ter concretisering van de wettelijke normstelling: Stuurman 2009, Kosta & Stuurman 2015 en Stuurman 2017.
590. HR 15 april 1994, NJ 1994, 608 (Valkenhorst), m.nt. Hammerstein-Schoonderwoerd.
591. HR 9 september 2011. LJN: BQ8097. JPG 2011/186.

Hoge Raad er uitdrukkelijk op dat in alle in artikel 8 Wbp genoemde mogelijke grondslagen de eis van 'noodzakelijkheid' is opgenomen. Dat wil zeggen dat niet alleen getoetst moet worden of de in artikel 8 Wbp genoemde redenen van verwerking van persoonsgegevens zich voordoen, maar ook of de voorgenomen verwerking in concreto wel noodzakelijk is. Vanuit het perspectief van informationele zelfbeschikking is van belang dat de verplichting tot belangenafweging in beginsel ook bestaat als de betrokkene toestemming heeft verleend.[592]

6.3.2 Dexia en Hollandsche Bank-Unie

Eind vorige eeuw boden verschillende banken, waaronder LegioLease en later de Dexia Bank, beleggingsproducten aan, aangeprezen als de 'winstverdubbelaar' en zelfs de 'winstverdriedubbelaar'. Dit betrof producten waarbij consumenten geld van de bank leenden die daarmee vervolgens voor hen aandelen kocht. Zolang de aandelenkoersen stegen kon zo een heel behoorlijk rendement worden gerealiseerd, wat leidde tot een grote populariteit van deze producten. Uiteindelijk ging het mis. De aandelenmarkten zakten in en veel afnemers van deze beleggingsproducten kwamen erachter dat zij, naar eigen zeggen zonder het te weten, grote schulden hadden opgebouwd. Om zich voor te bereiden op een procedure tegen de bank deed een aantal van hen een op artikel 35 Wbp gebaseerd verzoek om verstrekking van een overzicht van de persoonsgegevens die Dexia over hen verwerkte. In voorkomende gevallen maakten zij daarbij gebruik van een voorbeeldbrief die de programmamakers van Tros Radar op het internet beschikbaar stelden. De bank weigerde om een aantal redenen aan deze kennisnemingsverzoeken te voldoen. Aan de verschillende rechtbanken, gerechtshoven en ten slotte de Hoge Raad, werd vervolgens voorgelegd in hoeverre deze weigering terecht was.

De Hoge Raad beantwoordt deze rechtsvraag in drie arresten, waarvan er twee gaan over Dexia en één over de Hollandsche Bank-Unie of HBU. De relevante overwegingen in de drie arresten zijn grotendeels gelijkluidend, zij het dat het arrest over HBU een wat beperktere omvang heeft dan de beide Dexia-arresten. Informationele zelfbeschikking is terug te vinden in de genoemde drie beschikkingen.[593] Volgens de Hoge Raad zijn de banken als verantwoordelijken en verwerkers van persoonsgegevens verplicht desgevraagd aan betrokkenen van wie persoonlijke gegevens zijn verwerkt en opgeslagen, toegang te verschaffen tot de persoonsgegevens.

6.3.3 Universitair Medisch Centrum Groningen

Het Universitair Medisch Centrum Groningen (UMCG) heeft het verzoek van een patiënt om op grond van de Wbp kennis te nemen van de namen van de zorgverleners die inzage in haar elektronische medisch patiëntendossier hebben

592. Als bedoeld in artikel 8, aanhef en onderdeel a, Wbp.
593. HR 29 juni 2007, LJN: AZ4663 (Dexia), LJN: AZ4664 (Dexia) en LJN BA3529 (Hollandse Bank-Unie). Zie over deze arresten ook E. Thole e.a. (red.), 50 Vragen over privacy. Deventer: Kluwer, 2010, p. 150-153.

genomen, afgewezen. Het UMCG heeft het door de patiënt daartegen gemaakte bezwaar ongegrond verklaard.
De Afdeling Bestuursrechtspraak van Raad van State redeneerde dat 'raadplegen' niet hetzelfde is als 'verstrekken' van persoonsgegevens en dat 'raadplegers' of 'geautoriseerden' geen 'ontvangers' zijn.[594]

Deze redenering werd bekritiseerd door Overkleeft-Verburg. De wetgever lijkt namelijk nooit te hebben bedoeld om een juridisch relevant onderscheid te maken tussen het opvragen, raadplegen en verstrekken van persoonsgegevens. Voor informationele zelfbeschikking is bij deze uitspraak van belang dat dat Raad van State blijkbaar verder gaat dan de Hoge Raad – en de Wbp – in het toekennen van zelfbeschikking aan de patient over de namen van de zorgverleners die zijn elektronisch medisch dossier hebben ingezien.

6.3.4 Landelijk schakelpunt

Op 1 december 2017 heeft de Hoge Raad de uitspraken van Hof Arnhem-Leeuwarden van 8 maart 2016 en Rechtbank Midden-Nederland van 23 juli 2014 bekrachtigd.[595] Daarmee bevestigde de Hoge Raad dat het delen van patiëntgegevens via het Landelijk Schakelpunt (LSP) in overeenstemming is met de wet- en regelgeving omtrent de bescherming van persoonsgegevens en de bescherming van het medisch beroepsgeheim. De uitspraak van de Hoge Raad is het voorlopige sluitstuk in een juridische strijd die de Vereniging voor Praktijkhoudende huisartsen (VPH) samen met enkele patiënten heeft gevoerd tegen de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ). De VPH verzette zich destijds al nadrukkelijk tegen het voorstel voor de wet over het landelijke EPD, die in 2011 door de Eerste Kamer werd verworpen. Het LSP kende vervolgens in 2012 een doorstart door de koepels van huisartsen, de Landelijke Huisartsen Vereniging (LHV), huisartsenposten (InEen), apotheken via de Koninklijke Maatschappij ter bevordering van de Pharmacie (KNMP) en de Nederlandse Vereniging van Ziekenhuizen (NVZ). Ook daartegen heeft de VPH zich steeds verzet, onder meer door het voeren van deze juridische procedures.

Het LSP maakt het mogelijk dat zorgaanbieders toegang hebben tot bepaalde gegevens uit medische dossiers die door andere zorgaanbieders worden beheerd. Het regelt de toegangscontroles van alle aangemelde patiëntendossiers, registreert waar patiëntengegevens opvraagbaar zijn, welke gegevens zijn opgevraagd en door wie dat is gedaan. Vrijwel alle huisartsen stellen via het LSP een deel van het medisch dossier (de 'professionele samenvatting') elektronisch beschikbaar voor raadpleging door een waarnemend huisarts op de huisartsenpost. Van die toegang wordt gebruikgemaakt ten behoeve van de acute huisartsenzorg tijdens avond-, nacht- en weekenduren. Naast huisartsen stelt het overgrote deel van de apotheken via het LSP een overzicht van verstrekte medicatie ('het medicatiedossier') elektronisch beschikbaar voor raadpleging door (waarnemend) huisartsen,

594. ABRvS 30 november 2011, ECLI:NL:RVS:2011:BU6383, JB 2012/44 met annotatie van prof. mr. G. Overkleeft-Verburg.
595. HR 1 december 2017, ECLI:NL:HR:2017:3053.

bijvoorbeeld op de huisartsenpost, (poli-)apotheken en medisch specialisten (in ziekenhuizen en andere instellingen).

De Hoge Raad bevestigt in het arrest dat patiënten uitdrukkelijke toestemming moeten geven voordat zorgaanbieders via het LSP gegevens uit hun medische dossiers beschikbaar mogen stellen voor elektronische raadpleging door andere zorgaanbieders. Doordat gegevens uit het medisch dossier uitsluitend worden gedeeld na het geven van uitdrukkelijke toestemming door patiënten, oordeelt de Hoge Raad (in navolging van het hof, Rechtbank Midden-Nederland en de AP), dat raadplegingen die via het LSP plaatsvinden niet in strijd zijn met het medisch beroepsgeheim van zorgaanbieders. Sinds de inwerkingtreding van de Wabvpz op 1 juli 2017, is het wettelijk verplicht om vooraf toestemming te verkrijgen van patiënten om gegevens uit hun medische dossiers elektronisch beschikbaar te mogen stellen voor raadpleging door andere zorgaanbieders, voor zover daarbij gebruik wordt gemaakt van een 'elektronisch uitwisselingssysteem'.
Uitdrukkelijke toestemming alleen is echter niet voldoende voor een rechtmatige verwerking van patiëntgegevens. De VPH stelde dat ondanks de verkregen toestemmingen het delen van gegevens via het LSP niet voldoet aan de juridische eisen van proportionaliteit en subsidiariteit. De Hoge Raad verwerpt die stelling echter door erop te wijzen dat voor het LSP gebruik wordt gemaakt van algemene professionele standaarden die door de beroepsgenoten al sinds 1998 worden gehanteerd in waarneemsituaties. Deze standaarden beschouwt de Hoge Raad als een beoordeling van de vraag welke gegevens in het algemeen voor een goede zorgverlening bij spoedeisende hulp of waarneming van belang zijn, welke beoordeling op de praktijkervaring van de huisartsen is gebaseerd. Op basis daarvan oordeelt de Hoge Raad dat de gegevensverwerking via het LSP ook voldoet aan de eisen van proportionaliteit en subsidiariteit. Niet in elke situatie zal het noodzakelijk zijn om toegang te hebben tot alle beschikbare gegevens. Maar de Hoge Raad wijst erop dat dit inherent is aan het samenstellen van een algemene standaard. Bovendien hebben patiënten het recht om in overleg met de huisarts informatie uit te sluiten van raadpleging door andere opvragende zorgverleners.

Een ander onderdeel van het cassatieberoep dat de Hoge Raad verwerpt, is dat er bij gebruikmaking van het LSP geen sprake zou zijn van door de patiënten in vrijheid gegeven toestemming. Volgens de Hoge Raad is het hof op dit punt niet van een onjuiste rechtsopvatting uitgegaan. Het hof en de rechtbank waren van oordeel dat bij het LSP sprake is van toestemming zonder dwang. Dit oordeel berust op waarderingen van feitelijke aard, waardoor de Hoge Raad deze in cassatie niet op juistheid kan onderzoeken. Maar de Hoge Raad vindt dat oordeel niet onbegrijpelijk of onvoldoende gemotiveerd. Tot slot wijst de Hoge Raad erop dat de VPH de stelling dat de dwang om toestemming te verlenen zou voortkomen uit vrees voor een mogelijk minder goede medische behandeling, niet eerder bij de rechtbank en het hof hebben aangevoerd en dus ook niet tot cassatie kan leiden.

Ook het onderdeel dat de toestemming van patiënten onvoldoende specifiek zou zijn, wordt door de Hoge Raad verworpen. De Hoge Raad vindt dat op dit punt ook niet is gebleken van een onjuiste rechtsopvatting door het hof. Het hof had de opvatting van de rechtbank overgenomen dat in de informatiebrochure voor patiënten duidelijk is omschreven voor welke situaties toestemming wordt verleend. Met de rechtbank is het hof van oordeel dat voor een voldoende specifieke wilsuiting niet nodig is dat degene die toestemming verleent op dat moment ook al bekend is met de inhoud van de gegevens die zullen worden uitgewisseld. Daar komt bij dat patiënten desgewenst delen van informatie kunnen laten afschermen, zodat deze niet gedeeld wordt met andere zorgverleners.

De Hoge Raad schaart zich overigens achter het oordeel van het hof dat ten tijde van de uitspraak patiënten nog onvoldoende keuzemogelijkheden hebben om aan te geven met welke typen zorgaanbieders hun patiëntengegevens via het LSP gedeeld mogen worden. Volgens het hof zou VZVZ ernaar moeten streven om patiënten die aan het LSP willen deelnemen zo veel mogelijk beslissingsvrijheid te geven, zodat zij zo veel mogelijk regie hebben over het systeem. Hetgeen het hof heeft overwogen over wat van VZVZ mag worden verwacht, moet volgens de Hoge Raad als volgt worden begrepen. De inrichting van de zorginfrastructuur is op dit moment aanvaardbaar omdat zij berust op in vrijheid gegeven, voldoende specifieke toestemming van de betrokken patiënten. Het hof heeft daarbij echter onderkend dat de zorginfrastructuur ook kan worden ingericht op een wijze waarbij meer onderscheid tussen (soorten) gegevens en (categorieën) zorgaanbieders kan worden gemaakt, en waarbij in het bijzonder gegevensuitwisseling op basis van toestemming bij voorbaat desgewenst kan worden beperkt tot spoedeisende gevallen. Een dergelijke inrichting zou meer en beter in overeenstemming zijn met de beginselen die aan de Wbp ten grondslag liggen, maar deze konden ten tijde van het wijzen van het bestreden arrest nog niet van VZVZ worden geëist. De Hoge Raad vindt het niet onbegrijpelijk dat het hof van VZVZ verwacht dat zij, zodra dit voor haar technisch mogelijk en uitvoerbaar is, het systeem aanpast door daarin meer keuzevrijheid te bieden. Met deze uitspraak loopt de Hoge Raad – net als het hof en de rechtbank – de facto vooruit op de wettelijke eis van 'gespecificeerde toestemming' in de Wabvpz van 1 juli 2017, welke verplichting bij de inwerkingtreding van de wet is uitgesteld tot 1 juli 2020. De Hoge Raad doet in navolging van het hof terecht nog de aanbeveling – gelet op de ambities van VZVZ en de veranderingen in de wet- en regelgeving (zie daarvoor de conclusie van de advocaat-generaal onder 8.15-8.19) - '*privacy by design*' en 'privacy by default' uitdrukkelijk tot uitgangspunt te nemen overeenkomstig artikel 25, lid 1 en 2, AVG.

Met zijn uitspraak bevestigt de hoogste Nederlandse rechter, in navolging van Hof Arnhem-Leeuwarden en Rechtbank Midden-Nederland, de rechtmatigheid van het delen van gegevens uit patiëntendossiers door middel van het elektronische uitwisselingssysteem LSP.[596]

596. Zie annotatie van Hooghiemstra & Nouwt, 2018, JBP 2018/4.

6.3.5 Tuchtzaken

Niet alleen de uitspraken van reguliere rechters zijn relevant voor informationele zelfbeschikking in de zorg. Gezien de medische context dient ook de medische tuchtrechtspraak behandeld te worden.

Zo was informationele zelfbeschikking aan de orde in een uitspraak van het Regionaal Tuchtcollege 's-Gravenhage van 5 juli 2011.[597] In deze zaak werd een arts onder andere verweten dat zij tekort is geschoten door een deel van een origineel huisartsendossier te vernietigen zonder daarvan een kopie of scan beschikbaar te houden. Het College legde de arts hiervoor een waarschuwing op. De arts had zijn informatie niet eigenhandig mogen vernietigen.

In de uitspraak van het Centraal Tuchtcollege voor de Gezondheidszorg (CTG) van 26 januari 2010[598]overweegt het college dat een arts ten onrechte dacht dat tegenover de verplichting van de arts om een afschrift van het dossier te verstrekken, de verplichting van de patiënt staat om de rekening voor de ingreep te betalen. De patiënt had recht op afschrift van het dossier 'binnen redelijke termijn'. De patiënt mocht er op ieder moment voor kiezen het dossier op te vragen en het niet nakomen van zijn betalingsverplichting maakte hierop geen uitzondering.

Een ander voorbeeld waarin informationele zelfbeschikking een rol lijkt te spelen, is een uitspraak waarin een internist een waarschuwing wordt opgelegd voor het verstrekken van een oordeel over een patiënt aan het UWV.[599] De klacht luidde dat de internist niet aan het UWV had mogen doorgeven dat er zijns inziens geen bezwaren waren tegen het stapsgewijs hervatten van werkzaamheden door diens patiënt. Onder verwijzing naar de KNMG Richtlijn[600] oordeelt het tuchtcollege dat een oordeel over het hervatten van werkzaamheden aan specifieke deskundigen moet worden overgelaten, in casu de UWV-arts, en vooral niet aan de behandelaar. Met andere woorden gaat het er in deze uitspraak om dat een behandelend arts geacht wordt geen geneeskundige verklaringen over eigen patiënten te verstrekken. De behandelend arts dient de vertrouwensrelatie met de patiënt niet op het spel te zetten. Bovendien is de behandelend arts in de regel onbekend met de criteria die gelden om te kunnen beoordelen of iemand wel of niet geschikt is om bepaalde dingen wel of niet goed te kunnen doen, zoals goed voor de kinderen zorgen, een auto besturen of naar school gaan.

597. RTG 's-Gravenhage 5 juli 2011, LJN YG1213.
598. CTG 26 januari 2010. GJ 2010/38/JPG 2010/81.
599. RTC Zwolle, 10 mei 2012. LJN YG2019. JPG 2012/113.
600. KNMG Richtlijn 'omgaan met medische gegevens', 2010. Inmiddels is er een nieuwe richtlijn van de KNMG van 2016.

6.3.6 Autoriteit persoonsgegevens

De AP heeft een aantal adviezen uitgebracht en onderzoeken verricht over informationele zelfbeschikking bij het gebruik van gezondheidsgegevens. Voor deze dissertatie worden hier een aantal relevante uitspraken uitgelicht.

Voorafgaand aan de komst van persoonlijke gezondheidsomgevingen speelde in Nederland het vraagstuk in hoeverre het BSN in de zorg gebruikt mocht worden om dossiers aan elkaar te koppelen, gevolgd door het LSP. Het College bescherming persoonsgegevens (CBP), de rechtsvoorganger van de AP, heeft hierover verschillende uitspraken gedaan. Over het gebruik van het BSN in de zorg is het CBP speciaal benaderd en om advies gevraagd door de minister van VWS toen het Besluit 'gebruik burgerservicenummers in de zorg' werd aangescherpt.[601]

Ook over het LSP heeft het CBP zich uitgelaten en een definitief rapport uitgebracht, waarin het concludeerde dat er voldoende technische en organisatorische waarborgen waren getroffen om te bewerkstelligen dat alleen persoonsgegevens werden verwerkt van patiënten die daarvoor toestemming hadden verleend overeenkomstig de Wbp.[602]

Informationele zelfbeschikking met betrekking tot de bescherming van gezondheidsgegevens speelt eveneens ten aanzien van gegevens over zieke werknemers. Illustratief is wat dat betreft het rapport over verzuimreductie.[603] Naar aanleiding van een uitzending van het programma Zembla was door het CBP een onderzoek gestart. Het CBP concludeerde dat het verzuimbedrijf in strijd met de wet handelde door de wijze waarop het medische gegevens van zieke werknemers verzamelde ten behoeve van werkgevers. Uit het onderzoek blijkt dat zogeheten casemanagers gezondheidsgegevens opvroegen en daarbij verder gingen dan noodzakelijk was voor de verzuimbegeleiding van de zieke werknemers. Bovendien was medische informatie vaak ook toegankelijk voor werkgevers. Het CBP wees er met name op dat met het gebruik van toestemming als grondslag voor gegevensverwerking in een arbeidsrelatie terughoudend moet worden omgegaan.[604]
Een ander voorbeeld van een onderzoek naar schending van de Wbp met betrekking tot gezondheidsgegevens, is de opslag van gepseudonimiseerde gezondheidsgegevens bij collega-toezichthouder Nederlandse Zorgautoriteit (NZa).[605]

601. College bescherming persoonsgegevens aan de minister van VWS, d.d. 20 november 2006, kenmerk z2006-01388, advies inzake aanvulling Besluit gebruik burgerservicenummer in de zorg.
602. College bescherming persoonsgegevens, *Zienswijze CBP over doorstartmodel voor landelijke uitwisseling medische gegevens*, 9 augustus 2011 en CBP *Rapport definitieve bevindingen Landelijk Schakelpunt,* d.d. 1 september 2014, kenmerk z2012-779.
603. College bescherming persoonsgegevens. *Onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim door VCD Humannet B.V.* December 2014, kenmerk z2012-0028.8.
604. Zie ook de uitspraak van de AP over het verwerken van gezondheidsgegevens door werkgevers via wearables: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet.
605. Autoriteit Persoonsgegevens. *Rapport definitieve bevindingen NZa-DIS,* d.d. 13 september 2016, kenmerk z2015-00355.

In de regel heeft de AP tot op heden weinig sancties opgelegd. De AP gaf in plaats daarvan doorgaans aanwijzingen hoe de Wbp niet langer te schenden of gedoogde de situatie. Inmiddels heeft de rechter geoordeeld dat de AP meer handhavend zal moeten optreden. Die noodzaak volgt ook uit de aantoonplicht van artikel 5, lid 2, AVG en de zwaardere sancties die de AP op grond van de AVG kan opleggen.

6.3.7 Inspectie Gezondheidszorg en Jeugd

De Inspectie Gezondheidszorg en Jeugd (IGJ) houdt onder andere toezicht op medische hulpmiddelen op grond van een Europese richtlijn, die vervangen wordt door de Verordening voor medische hulpmiddelen.[606] In de nieuwe verordening wordt een medisch hulpmiddel als volgt gedefinieerd:

> "medisch hulpmiddel": een instrument, toestel of apparaat, software, implantaat, reagens, materiaal of ander artikel dat of die door de fabrikant is bestemd om alleen of in combinatie te worden gebruikt bij de mens voor een of meer van de volgende specifieke medische doeleinden:
> – diagnose, preventie, monitoring, voorspelling, prognose, behandeling of verlichting van ziekte,
> – diagnose, monitoring, behandeling, verlichting of compensatie van een letsel of een beperking,
> – onderzoek naar of vervanging of wijziging van de anatomie of van een fysiologisch of pathologisch proces of een fysiologische of pathologische toestand,
> – informatieverstrekking via in vitro-onderzoek van specimens afkomstig van het menselijk lichaam, waaronder orgaan-, bloed- en weefseldonaties, waarbij de belangrijkste beoogde werking in of op het menselijk lichaam niet met farmacologische of immunologische middelen of door metabolisme wordt bereikt, maar wel door die middelen kan worden ondersteund.
> De volgende producten worden eveneens aangemerkt als medische hulpmiddelen:
> – hulpmiddelen voor de beheersing of ondersteuning van de bevruchting;
> – producten die speciaal bestemd zijn voor het reinigen, ontsmetten of steriliseren van hulpmiddelen bedoeld in artikel 1, lid 4, en van die bedoeld in de eerste alinea van dit punt.

Op dit moment ziet de IGJ toe op de Wet op de medische hulpmiddelen en het Besluit Medische Hulpmiddelen. Een softwareproduct is een medisch hulpmiddel als het een diagnostische of therapeutische functionaliteit heeft. Persoonlijke gezondheidsomgevingen zijn geen medische hulpmiddelen[607] zolang daarin alleen gezondheidsgegevens worden opgeslagen. De AP is dan toezichthouder op de bescherming van de gezondheidsgegevens. Zodra persoonlijke gezondheidsomgevingen een diagnostische of therapeutische functionaliteit hebben zijn het wel medische hulpmiddelen. Van de 350.000 gezondheidsapps zijn er diverse met een diagnostische of therapeutische functionaliteit en als ze het nog niet hebben, dan is er vaak wel de potentie toe. Vele persoonlijke gezond-

606. EU Verordening van 5 april 2017, nr. 2017/745 (betreffende medische hulpmiddelen).
607. In het algemeen wordt aangenomen dat een patiënt met een leverancier van medische hulpmiddelen ook geen geneeskundige behandelingsovereenkomst sluit en leveranciers van medische hulpmiddelen op basis van een dergelijke overeenkomst niet gebonden zijn aan de in de WGBO opgenomen patiëntenrechten, zie Ploem & Dute 2014.

heidsomgevingen vallen daarmee zowel onder het toezicht van de AP als van de IGJ. Softwareproducten met een medisch doel moeten zijn aangemeld als medisch hulpmiddel en een CE-markering hebben.[608] Een CE-markering geeft aan dat het product voldoet aan een aantal essentiële eisen[609]. Sinds 1 januari 2014 treedt de IGJ op als softwarefabrikanten zich niet aan de Wet op de medische hulpmiddelen houden. Ook vraagt de IGJ technische dossiers op bij de fabrikant als zij een risico vermoedt bij een bepaald product.

De softwareproducten in de gezondheidszorg worden almaar intelligenter en krijgen een steeds prominentere rol in het zorgproces. Deze vernieuwing heeft potentiële risico's voor de persoon als die software niet goed functioneert en bijvoorbeeld een foute diagnose genereert. Zowel tijdens het ontwikkel- en implementatieproces als tijdens het gebruik van software kunnen fouten optreden. Het is de verantwoordelijkheid van zorgverleners, fabrikanten en personen om goed met deze risico's om te gaan.

6.4 CONCLUSIE NEDERLAND

Dit hoofdstuk startte met de vraag in hoeverre – in het licht van de eerste en tweede onderzoeksvraag – de Nederlandse regulering voldoende anticipeert op maatschappelijke en technologische ontwikkelingen rond informationele zelfbeschikking binnen en buiten de zorgcontext. Deze vraag behoeft meer specifiek beantwoording in het licht van de centrale thematiek van deze dissertatie, namelijk de vraagstukken rond de in opkomst zijnde persoonlijke gezondheidsomgevingen.

In Nederland blijkt er geen algemeen recht op informationele zelfbeschikking te bestaan, ondanks meerdere pogingen een dergelijk recht te realiseren. Vooralsnog is in Nederland ook geen recht op informationele zelfbeschikking in zicht. Vanwege het samenspel met artikel 8 EVRM is in de literatuur impliciet uit artikel 10 Grondwet informationele zelfbeschikking afgeleid. De staatscommissie Grondwet heeft in 2010 een zelfstandige Grondwetsbepaling voor informationele zelfbeschikking voorgesteld. Het is de vraag of een Grondwetsbepaling voor informationele zelfbeschikking nog relevant is nu dit hele domein dwingend EU-recht is. In het vorige hoofdstuk over privacy en gegevensbescherming in Europa kwamen de informationele zelfbeschikkingsrechten uit de AVG binnen de gehele Europese Unie aan de orde. Privacy en gegevensbescherming 'wortelen' in de oude Nederlandse klassieke grondrechten en de lange traditie van het medisch beroepsgeheim. Specifiek voor de Nederlandse situatie bestaan er op dit moment – binnen de bestaande zorgcontext – actieve, afzonderlijke, 'informationele zelfbeschikkingsrechten', die met name te vinden zijn in de WGBO en in het bijzonder in de Wabvpz die 1 juli 2017 in werking is getreden, met een overgangstermijn van drie jaren voor de nieuwe, actieve zelfbeschikkingsrechten 'elektronische inzage' en 'gespecificeerde toestemming'.

608. Zie RVZ 2015 en Van der Mersch, 2018.
609. Voor een nadere definiering van de CE-markering, zie het rapport van de Algemene Rekenkamer (2016).

Bij de WGBO blijkt het binnen de geneeskundige behandelingsovereenkomst daarnaast te gaan om informationele zelfbeschikkingsrechten als het recht op niet weten, de dossierplicht van de hulpverlener, bewaartermijnen, recht op vernietiging, recht op inzage en afschrift en het medisch beroepsgeheim.

Artikel 30 van de UAVG behandelt uitzonderingen op het verbod om gezondheidsgegevens te mogen verwerken. Verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen mogen met uitdrukkelijke toestemming van de betrokken persoon (gebruiker) gezondheids- en andere gegevens van de persoon verwerken.

Voor verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen geldt op grond van de (U)AVG geen wettelijke zwijgplicht, zoals medische hulpverleners die hebben in de zin van de Wet BIG en de WGBO. Ook hebben zowel de verwerkingsverantwoordelijken van persoonlijke gezondheidsgegevens als de betrokken personen geen verschoningsrecht in de zin van artikel 218 Sv.

De Nederlandse rechtspraak laat in paragraaf 6.3 een genuanceerd beeld zien ten aanzien van de ontwikkeling van informationele zelfbeschikkingsrechten in de Nederlands zorg, waarbij er geleidelijk aan sprake is van een ontwikkeling van 'negatieve' afweerrechten naar 'positieve' participatierechten.
Uit de zaak Satander, paragraaf 6.3.1, blijkt dat het informationele zelfbeschikkingsrecht 'toestemming' in Nederland een belangenafweging vergt gelet op de eis van 'noodzakelijkheid'.De Hoge Raad en het Hof Arnhem-Leeuwarden zijn in de zaak over het Landelijk Schakelpunt, paragraaf 6.3.4, vooruitgelopen op de Wabvpz die 1 juli 2017 in werking is getreden, met een overgangstermijn van drie jaren voor het nieuwe recht op 'gespecificeerde toestemming' bij elektronische gegevensuitwisseling tussen zorgaanbieders. De Hoge Raad en het Hof vinden dat cliënten meer keuzevrijheid zouden moeten krijgen door zodra het technisch mogelijk en uitvoerbaar is de zorginfrastructuur in te richten op een wijze waarbij meer onderscheid tussen (soorten) gegevens en (categorieën) zorgaanbieders kan worden gemaakt, en waarbij in het bijzonder gegevensuitwisseling op basis van toestemming bij voorbaat desgewenst kan worden beperkt tot spoedeisende gevallen. Informationele zelfbeschikking blijkt zich bij uitwisseling van gezondheidsgegevens tussen zorgaanbieders ook in de rechtspraak van 'negatieve' afweerrechten naar 'positieve' participatierechten te ontwikkelen.

Buiten de behandelrelatie tussen zorgaanbieder en patiënten/cliënten blijkt de wetgever nog niet of nauwelijks te anticiperen op de komst van persoonlijke gezondheidsomgevingen (websites en *apps*) die – doorgaans buiten de zorgsector opererende – (commerciële) organisaties met mogelijk veel 'datamacht' ter beschikking stellen aan mogelijk kwetsbare personen. De AVG, de UAVG en de Wabvpz laten deze ontwikkeling buiten beschouwing. Dat betekent dat de wetgever onvoldoende anticipeert op de toenemende invloed van private aan-

bieders[610], maar ook op de groeiende invloed van de overheid[611]. Vandaar dat in het volgende hoofdstuk over rechtsbescherming wordt bezien hoe de geconstateerde transformatie van informationele zelfbeschikking binnen de zorg – van 'negatieve' afweer naar een 'positieve' participatie – ook buiten de behandelrelatie gepaard kan en zou moeten gaan met adequate regulering ter bescherming van personen tegen misbruik, zoals oneigenlijke toegang tot of verkoop van gezondheidsgegevens. Ook komt in het volgende hoofdstuk aan de orde hoe zowel vanuit toezichthouders als vanuit het gebruikersperspectief op praktische wijze rechtsbescherming mogelijk is tegen – ondoorzichtige – gebruikshandelingen met betrekking tot gezondheidsgegevens.

610. Zie paragraaf 2.6.
611. Zie paragraaf 2.7.

7. *Rechtsbescherming*

7.1 INLEIDING

Uit de voorgaande hoofdstukken blijkt dat er een fundamentele verschuiving in het denken over het begrip 'informationele zelfbeschikking' gaande is. Het gaat om een transformatie van 'negatieve' afweer naar 'positieve' participatie. Recentelijk krijgt het begrip een positieve, actieve lading: de betrokken 'personen'[612] zouden zelf het heft in handen moeten kunnen krijgen. Bijvoorbeeld via persoonlijke gezondheidsomgevingen die met behulp van websites en apps toegang gaan bieden aan alle gezondheidsgegevens van de betrokken persoon. Er is sprake van een explosief aanbod van technologie en applicaties, die mogelijkheden scheppen om 'informationele zelfbeschikking' daadwerkelijk, actief en assertief vorm te geven.

Net als bij andere technologische vernieuwingen biedt het nieuwe speelveld kansen en zorgt het voor risico's. Er ontstaan ruimere mogelijkheden, maar de traditionele normatieve mechanismen worden uitgedaagd. Voor sommige typen personen zullen de nieuwe mogelijkheden aantrekkelijk en zinvol zijn. De ruimere beschikbaarheid van gezondheidsgegevens roept echter ook fundamentele vragen op.

Gezondheidsgegevens worden al lange tijd gekwalificeerd als 'bijzondere of gevoelige gegevens', die extra zorg en bescherming verdienen. Al lang voor de moderne regulering van privacy en de bescherming van persoonsgegevens gold het medisch beroepsgeheim met de bijhorende zwijgplicht en het verschoningsrecht, dat door medische beroepsbeoefenaren en door de rechter strikt werd opgevat. Inmiddels staan het medisch beroepsgeheim en de bijbehorende zwijgplicht en het verschoningsrecht voor hulpverleners – mede onder invloed van de in de voorgaande hoofdstukken beschreven maatschappelijke en technologische ontwikkelingen – steeds meer onder druk. Wanneer personen daadwerkelijk de eigen gezondheidsgegevens gaan 'beheren', valt de van oudsher bestaande bescherming van het medisch beroepsgeheim zelfs grotendeels[613] weg.

612. Synoniem voor: individu, gebruiker, betrokkene, patiënt, cliënt, zorgconsument en werknemer.
613. Zie paragraaf 3.4. waaruit blijkt dat in het wetsvoorstel tot vaststelling van het nieuwe artikel 218 Sv wordt voorgesteld dat het verschoningsrecht zich ook uitstrekt tot de informatie van verschoningsgerechtigden in een persoonlijke gezondheidsomgeving, waardoor het medisch beroepsgeheim ten aanzien van het verschoningsrecht niet helemaal weg zou vallen als personen hun 'eigen' gezondheidsgegevens 'beheren'. De zwijgplicht van het medisch beroepsgeheim vervalt ook in dat geval voor de informatie in de persoonlijke gezondheidsomgeving indien de verwerkingsverantwoordelijke voor het beheer van de persoonlijke gezondheidsomgeving buiten de geneeskundige behandelingscontext staat.

Tegelijkertijd kunnen zowel publieke als private organisaties misbruik of oneigenlijk gebruik maken van deze als gevoelig gekarakteriseerde gegevens. Dit betekent dat er denkwerk moet worden verricht om een beproefde functie van het recht – namelijk het op een ordelijke en behoorlijke wijze stroomlijnen van sociale, economische en technologische veranderingen[614] – ook in het geval van deze ontwikkelingen waar te kunnen maken. Hoe kunnen we de rechtsbescherming voor de betrokkenen op een verantwoorde wijze vormgeven? Het gaat om 'werk in uitvoering', want de technologische en maatschappelijke vernieuwing verloopt turbulent en het recht dreigt daar achteraan te hinken.

Dit hoofdstuk probeert een zo helder mogelijke normatieve veldverkenning te bieden van arrangementen voor rechtsbescherming als bijdrage aan de gedachtevorming alsmede de rechtsvorming. Van te voren staat vast dat een compleet overzicht onmogelijk is. Het gaat om een reflectie op hoofdlijnen.

Vanuit deze doelstelling staan in dit hoofdstuk de derde en vierde onderzoeksvraag van deze dissertatie centraal:

> Onderzoeksvraag 3: Normering kan ook gestalte krijgen in de applicaties zelf, namelijk via *privacy-by-design*. Deze en andere mogelijkheden kunnen in potentie personen faciliteren bij het beheer van hun gezondheidsgegevens. Maar wat betekent dit concreet op het terrein van gezondheid en gezondheidszorg?
>
> Onderzoeksvraag 4: Welke overige toekomstgerichte aanbevelingen zijn er - gelet op de opmars van persoonlijke gezondheidsomgevingen - te geven om informationele zelfbeschikking te realiseren?

Bij het vormgeven van de rechtsbescherming dient voorop te staan dat het hier gaat om zulke ingrijpende technologische innovaties die zich in een zo hoog tempo voordoen, dat moet worden gestreefd naar een zoveel als mogelijk technische inbedding van rechtsbescherming. Zo zal op technisch ontwerpniveau in het licht van de derde onderzoeksvraag – anticiperend – moeten worden gewerkt met de mogelijkheden van *privacy by design* of – ruimer geformuleerd – *rechtsbescherming by design*.[615]

Eerder in deze dissertatie[616] is een aantal normatieve uitgangspunten ontwikkeld die in dit hoofdstuk nader worden vertaald en geconcretiseerd. Wat betreft het uitgangspunt van de menselijke waardigheid gaat het om de vraag wat dit inhoudt voor wet- en regelgeving. Dan gaat het bijvoorbeeld om de principiële kwestie van een aanvullend wettelijk te regelen zwijgplicht voor verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen en een verschoningsrecht voor betrokken (rechts)personen[617]. Of om de vraag onder welke

614. Kees Schuyt, Recht en Samenleving, 1983.
615. Bij de relatie tussen technologie en wetgeving kunnen twee invalshoeken worden onderscheiden te weten 'juridische bescherming by design' en '(computer)code as regulation', zie Hildebrandt, Leenes en Lokin, 2012 p. 61-75.
616. Hoofdstuk 3.
617. Zie bijvoorbeeld 1.5.3, 3.4. en 3.6.

voorwaarden leveranciers persoonlijke gezondheidsomgevingen mogen leveren. Te denken valt aan voorwaarden die specifiek beogen om misbruik te voorkomen. Wat betreft responsieve regulering gaat het om regels die begrijpelijk en toepasbaar zijn. Gebruikers moeten er zogezegd mee uit de voeten kunnen. Bij contextuele integriteit gaat het om de vraag of voldoende rekening wordt gehouden met de situatie van mensen die met de betreffende zorgtoepassing te maken krijgen. Met andere woorden, het gaat niet alleen om de persoonsgegevens als zodanig, maar ook om de specifieke situatie waarin de betreffende persoon zich bevindt. Daarbij is het goed om een aantal fasen te onderscheiden en te preciseren bij welke actoren de voornaamste juridische, technische en morele verantwoordelijkheden liggen.

Het gaat in dit hoofdstuk om rechtsbescherming in ruime zin, waarin de verantwoordelijkheid van ICT-aanbieders, zorgaanbieders en gebruikers van bijvoorbeeld persoonlijke gezondheidsomgevingen aan de orde komt. Daarbij is leidend de zoektocht naar een snelle en gebruiksvriendelijke weg naar rechtsbescherming in de gevallen waarin problemen, fricties of conflicten optreden. Essentieel daarbij is een realistische inschatting van de mogelijkheden van de (zelf)redzaamheid van mensen, zoals geagendeerd in het WRR-rapport '*Weten is nog geen doen*'[618]. Nuchterheid, behoedzaamheid en een realistisch inzicht in psychologische processen zijn geboden. 'De patiënt' of 'de persoon' bestaat niet in de praktijk. Om toch enigszins te bepalen in welke mate een persoon extra zelfbeschikking dient te krijgen over zijn gezondheidsgegevens zijn in paragraaf 2.1 daarom drie groepen personen onderscheiden waarvoor extra juridische en morele aandacht noodzakelijk is:

1. Degenen die zich zorgen maken over machtsmisbruik;
2. Degenen die gegevens niet kunnen of willen 'managen';
3. Degenen die actief zelf persoonsgegevens willen 'managen'.

Gegeven dit gedifferentieerde beeld mag niet van alle mensen verwacht worden dat zij gebruik kunnen en zullen gaan maken van de informationele zelfbeschikkingsmogelijkheden die in ontwikkeling zijn. Het is essentieel om vast te houden aan het principiële uitgangspunt dat men niet gedwongen mag worden tot het gebruik van de goedbedoelde mogelijkheden die ontwikkeld worden om personen meer informationele zelfbeschikking te bieden. Informationele zelfbeschikking mag immers niet verworden tot een plicht[619]. Zeker niet bij degenen die dat niet willen of kunnen. Er dient juist rekening te worden gehouden met omvangrijke groepen minder (digitaal) vaardige gebruikers. Zo blijkt uit de Sociale Staat van Nederland 2017 van het Sociaal Cultureel Planbureau (SCP) dat digitale vaardigheden van belang zijn voor het kunnen uitoefenen van regie over het eigen leven en dat velen niet digitaal vaardig zijn.[620] Ongeveer 11% van de Nederlanders van 16 tot 65 jaar heeft geen of weinig ervaring met de computer.[621] Bij 65-75 jarigen

618. WRR 2017.
619. In vorige golven van informatisering zijn goed bedoelde mogelijkheden regelmatig verworden tot een plicht.
620. SCP 2017, p. 351, tabel 12.8.
621. https://www.rijksoverheid.nl/onderwerpen/laaggeletterdheid/digitale-vaardigheden.

is dat 15% en 75-plussers (50%).[622] Naast ouderen hebben ook lager opgeleiden, allochtonen en inactieven lagere digitale vaardigheden, waarbij inkomen en opleiding de belangrijkste voorspellers zijn.[623] Wat de medische context hierbij bijzonder maakt, is dat juist wanneer mensen geconfronteerd worden met een ingrijpende, vaak existentiële, medische kwestie ook doorgaans vaardige en mondige personen soms machteloos en hulpeloos blijken te zijn.[624] De WRR wijst er in het rapport 'Weten is nog geen doen' eveneens op dat onder bepaalde omstandigheden (spanning, life events) vaardigheden aangetast raken.[625]

Met deze vaststelling wordt de vraag relevant, welke rol van de overheid en daarmee wetgever mag worden verwacht. In rechtstheoretische zin kan worden beargumenteerd dat minimaal liberaal legalisme met een kleine overheid, personen te weinig bescherming biedt, juist waar bescherming dringend noodzakelijk is. Tegelijkertijd waarschuwde Berlin dat een begrip als positieve vrijheid met een actieve overheid die vergaande verplichtingen oplegt het gevaar van ideologisch misbruik en politieke manipulatie op kan roepen. Eventuele risico's dienen zoveel mogelijk technologisch, organisatorisch of juridisch te worden weggenomen. Vertaald in praktische termen betekent dit dat zij die van deze mogelijkheden gebruik willen maken er op zouden moeten kunnen vertrouwen dat de toepassingen voldoen aan *privacy-by-design* en dat de overheid en de wetgever op deze ontwikkelingen anticipeert via beleid en wet- en regelgeving.

De zoektocht naar betekenisvolle informationele zelfbeschikking in de zorg leidt in dit hoofdstuk tot de beschrijving van normatieve kaders waarbinnen informationele zelfbeschikking zich dient af te spelen. Bij rechtsbescherming gaat het erom dat personen zoveel mogelijk in een positie komen te verkeren waarin zij daadwerkelijk over hun informatie kunnen beschikken. In een aantal recente publicaties wijzen auteurs erop dat de gegevens-infrastructuur zo ingewikkeld en ondoorzichtig is geworden dat een zinvolle invulling van het toestemmingsvereiste moeilijk, vaak zelfs onmogelijk wordt.[626] De ingewikkelde *policies* en algoritmen zijn voor de meeste personen niet te doorzien. Dat een zinvolle invulling van het toestemmingsvereiste vaak onmogelijk wordt, roept de vraag op welke aanvullende normatieve '*checks and balances*' geboden zijn. In hoofdstuk 2 is geconcludeerd dat er praktische en technologische mogelijkheden lijken te zijn om personen informationele zelfbeschikking te bieden, maar dat dit niet altijd en niet voor alle typen personen geldt. In de volgende paragraaf komt daarom de vraag aan de orde in hoeverre technologie mensen preventief kan helpen bij het uitoefenen van informationele zelfbeschikking.

622. CBS Statline, gegevens 2015.
623. SCP 2107.
624. Zie de figuur in 1.5.3.
625. WRR, 2017.
626. WRR 2011: Het individu wordt steeds zichtbaarder, behalve voor zichzelf, Moerel, 2014 p.47-50 en Moerel & Prins 2016, p. 20.

Gelet op de zeer complexe gegevens-infrastructuur en de precaire status van het toestemmingsvereiste door (zorg)gebruikers, is een verschuiving nodig van de verantwoordelijkheid voor het realiseren van beschikking over de eigen informatie door de (zorg)gebruiker naar de wet- en regelgever en ontwerpers van persoonlijke gezondheidsomgevingen. Om een zorgvuldige toepassing van 'informationele zelfbeschikking' mogelijk te maken, zal de verantwoordelijkheid van bedrijven en overheidsinstanties geactiveerd moeten worden. Behalve dat bedrijven, overheden en zorgaanbieders actief hun verantwoordelijkheid nemen, moeten personen als zorggebruikers ook zelf mogelijkheden krijgen om met behulp van digitale hulpmiddelen informationele zelfbeschikking te bevorderen. Dat zou bijvoorbeeld kunnen gebeuren via een 'digitale butler'. Een digitale butler kan de afgifte van persoonsgegevens aan de hand van de voorkeuren van de gebruiker automatisch beschermen bij transacties tussen personen en bijvoorbeeld leveranciers van persoonlijke gezondheidsomgevingen en zorgaanbieders.

In dit hoofdstuk over rechtsbescherming in ruime zin keer ik ook weer terug op het reeds in paragraaf 3.3. besproken werk van de rechtssociologen Nonet & Selznick: '*Law and Society in Transition: Towards Responsive Law*'. Nonet en Selznick onderscheiden de volgende drie ideaaltypische vormen van het recht: 1. Repressief recht: het recht als instrument van de politieke elite; 2. Autonoom recht: het recht als tegenhanger van de politiek, waarbij machtsmisbruik wordt tegengegaan met behulp van rechtsbescherming in de vorm van regels en procedures; 3 Responsief recht: het recht met als doel het vergroten van de maatschappelijke rechtvaardigheid. Nonet en Selznick stellen dat deze drie ideaaltypen van recht opeenvolgende fasen in een evolutie vormen.[627] Responsief recht is volgens hen het meest ideaal, omdat in een systeem van responsief recht geen genoegen wordt genomen met rechtmatigheid, maar rechtvaardigheid de maatstaf is voor de legitimiteit van het recht . Hun pleidooi voor responsief recht betekent niet dat de rechtsbescherming van het autonoom en repressief recht zou moeten wegvallen. Ook autonome en repressieve rechtsbescherming blijven noodzakelijk.

In het navolgende manifesteert de rechtsbescherming zich op twee wijzen. Ten eerste in preventie, door te anticiperen op mogelijke problemen in ontwikkelingen die op ons afkomen. Ten tweede door autonome en repressieve rechtsbescherming. Responsief recht en responsieve rechtsbescherming houden in dat zowel in de ontwerp- als in de uitvoeringsfase, uitdrukkelijk rekening moet worden gehouden met de concrete leefwereld en beschermingsbehoefte van personen. Dat houdt ten eerste in dat ontwerpers een resultaatsverplichting[628] hebben om op mogelijke problemen te anticiperen. In de tweede plaats moet er een snelle, gebruiksvriendelijke en zorgvuldige manier zijn om praktische kwesties aan te kaarten.

627. Verberk, 2011.
628. Zie Borking, 2012. P.7: De verantwoordelijke kan wel de ontwerper of de bouwer van een systeem wegens wanprestatie aanspreken, wanneer de overeengekomen specificaties niet zijn toegepast, hetzij wanneer de bouwer door ontwerpfouten een onveilig systeem heeft opgeleverd dat inbreuken mogelijk maakt.

In aanvulling op responsief recht blijven autonome en repressieve macht ten opzichte van de machtige positie van bedrijven en overheden noodzakelijk. Sterke toezichthouders en een digitaal vaardige rechterlijke macht moeten aan de hand van stevige wet- en regelgeving optreden tegen malafide opererende bedrijven of overheden die misbruik maken van de afhankelijke positie waarin personen zich bevinden. Sommige mensen en organisaties hebben immers ook donkere kanten. Concreet is dit bijvoorbeeld zichtbaar in de verschillende manifestaties van het fenomeen cybercrime. Denk aan de wereldwijde aanval *Wannacry*, mei 2017, waarbij vooral ziekenhuizen in het Verenigd Koninkrijk getroffen werden.[629] Of denk aan het *Darkweb*[630], waar medische gegevens veel meer waard zijn dan creditkaartgegevens.

De eerstvolgende paragraaf gaat over de preventieve fase van rechtsbescherming aan de hand van *privacy-by-design* (subparagraaf 7.2.1).Daarna komt in subparagraaf 7.2.2. de in ontwikkeling zijnde zelfregulering in de vorm van het publiek-private Afsprakenstelsel MedMij aan de orde dat anticipeert op en voorwaarden stelt aan de komst van persoonlijke gezondheidsomgevingen. Bij MedMij gaat het om een afsprakenstelsel van leveranciers, zorgaanbieders en gebruikers van websites of *apps* waarmee een zorggebruiker idealiter integraal toegang heeft tot al zijn eigen gezondheidsgegevens. Paragraaf 7.3 gaat over responsieve probleem- en geschillenbehandeling. Bijvoorbeeld via *online dispute resolution* in de vorm van algoritmen, een ombudsfunctie, informatievertrouwenspersoon en mediators. Daarna volgt paragraaf (7.4) over de rechter en toezicht.

7.2 PREVENTIEVE FASE

7.2.1 Privacy-by-design

Het concept van *privacy-by-design* is nauw verwant aan het concept van *privacy enhancing technologies* (PET).[631] Het begrip PET houdt verband met het principe van 'dataminimalisatie' dat geleidelijk is verruimd tot het principe van '*privacy-by-design*'. PET is niet alleen relevant voor informatietechnologische systemen, maar ook voor organisaties, processen, governance en methoden in het algemeen.[632] Het concept van *privacy-by-design* wordt inmiddels wereldwijd gebruikt.[633]

629. 12 mei 2017, 'Waarschuwing voor grote internationale gijzelsoftware-campagne', nos.nl.
630. Ook wel *deepweb* genoemd, een onderdeel van het wereldwijde web dat niet rechtstreeks vindbaar is voor reguliere zoekmachines, maar uitsluitend via speciale software en wachtwoorden. Wordt naast journalisten, klokkenluiders en *cryptocurrencies* ook gebruikt door criminele en terroristische organisaties om moeilijk traceerbare illegale transacties te kunnen uitvoeren.
631. Zie Hes & Borking, 2010 met de revised edition van 1995.
632. P. Hustinx, *Privacy by design*: delivering the promises, in: Identity in the Information Society, August 2010, Volume 3, Issue 2, pp 253–255.
633. Ann Cavoukian (2009) formuleerde op basis van eerder werk van Kim Cameron (2005) zeven principes van *privacy by design. De voorgeschiedenis van privacy-by-design* is mooi beschreven door Christiane Schulzki in zeven delen en in het proefschrift van John Borking over *privacy-enhancing-technologies*.

Een eenduidige definitie van *privacy-by-design* ontbreekt.[634] Het beginsel *privacy-by-design* is in de loop van de jaren verruimd[635], onder andere door Van Lieshout[636] en Borking.[637]
Borking hanteert het begrip '*privacy-by-design*' liever dan '*data protection-by-design*':

> *"Privacybescherming is veel ruimer dan 'data protection'-bescherming. Het enkele feit dat er in mijn omgeving een 'stille' sensor is die uitsluitend wordt geactiveerd bij bepaald gedrag van mij en anders volledig 'mute' is, kan als een privacyschending ex artikel 8 Europese Verdrag tot Bescherming van de Rechten van de Mens (EVRM) worden beschouwd, maar niet als een schending van de AVG. Dat komt pas als deze sensor gegevens gaat verwerken."*

Privacy-by-design is enerzijds een verplichting opgelegd aan de verwerkingsverantwoordelijke en anderzijds is *privacy-by-design* voor de persoon die dat wil en kan ook een mogelijkheid om zichzelf te beschermen. Dat gaat verder dan de verplichtingen voor de verwerkingsverantwoordelijke in de AVG die nu eerst aan de orde komen.

Verplichtingen voor de verwerkingsverantwoordelijke
Wat betreft *privacy-by-design* als verplichting voor de verwerkingsverantwoordelijke is artikel 25 AVG relevant. In artikel 25 AVG is *privacy-by-design* geïntroduceerd als '*data protection-by-designand by default*'.

Een vereiste bij *data protection-by-design* is dat zo weinig mogelijk persoonsgegevens worden verwerkt. Nagegaan dient te worden óf en welke gegevens écht noodzakelijk zijn om het doel te bereiken. Daarbij dient ook nagedacht te worden over de vraag of persoonsgegevens van iedereen verwerkt moeten worden of dat op voorhand bepaalde groepen personen uitgesloten kunnen worden. Verder moeten ook gegevens worden verwijderd wanneer ze niet meer noodzakelijk zijn. Om *data protection-by-design* praktisch hanteerbaar te maken, zijn in de literatuur diverse benaderingen ontwikkeld en gedefinieerd.[638]

Een voorbeeld van *data protection-by-default* als verplichting voor de verwerkingsverantwoordelijke is de verplichting in Japan dat de *default* instelling van een smartphone standaard geen signalen[639] mag afgeven aan de buitenwereld. In Europa mag dit nog wel, wat leidt tot het permanent kunnen volgen van de houder van de smartphone door middel van WiFi-telling. In het licht van artikel 25 AVG is te bepleiten dat ook hier deze *default setting* verplicht wordt.

Motie-Bredenoord: dataprotectie-by-design bij elektronische verwerking medische gegevens
In subparagraaf 6.2.4 kwam de Wabvpz aan de orde. De Wabvpz is te beschouwen als een aanvulling op de AVG voor elektronische uitwisselingssystemen van zorgaanbieders die gezondheidsgegevens verwerken. Bij de behandeling van deze wet is de motie van het D66-Eerste Kamerlid Bredenoord over 'dataprotectie-

634. Borking 2013.
635. Cavoukian, 2009.
636. Van Lieshout, 2012.
637. Borking, 2013.
638. Zie Hustinx, 2010 en Hoepman, 2014, Colesky, Hoepman & Hillen, 2016 en Dickie & Yule, 2017.
639. Wifi, bluetooth etc.

by-design bij elektronische verwerking van medische gegevens' met algemene stemmen aangenomen.
Deze motie begon met de overweging dat bij de inrichting van een systeem voor de elektronische uitwisseling van medische gegevens de veiligheid voorop dient te staan. Geconstateerd werd dat de AVG bij de verwerking van persoonsgegevens vraagt om dataprotectie-by-design. Vandaar dat op grond van deze motie de Eerste Kamer de regering heeft verzocht 'dataprotectie-by-design' verder uit te werken als het uitgangspunt voor de elektronische verwerking van medische gegevens door zorgaanbieders en de Kamer daarover te informeren.

Digitale butler, algoritmes en certificering
Privacy-by-design kan dankzij kunstmatige intelligentie ook bijdragen aan informationele zelfbeschikking voor de persoon zelf – die dit wil en kan – met behulp van een persoonlijke assistent, oftewel een 'digitale butler'[640], via een nieuw institutioneel ontwerp.[641] Een voorbeeld van een digitale butler die personen als persoonlijke assistent kan helpen bij privacy- en gegevensbeschermingsvraagstukken werd in 2003 al beschreven in het handboek voor de *privacy incorporated software agent* (PISA).[642] De PISA is met EU geld ontwikkeld en wordt momenteel doorontwikkeld tot een een op de markt verkrijgbare digitale butler die de afgifte van persoonsgegevens aan de hand van de privacyvoorkeuren van de gebruiker automatisch kan beoordelen en afhandelen bij transacties tussen personen enerzijds en (software)leveranciers, bedrijven, overheden en instanties anderzijds. In de dagelijkse praktijk zijn er buiten 'privacy-by design-toepassingen' al vele digitale (meer of minder intelligente) butlers beschikbaar.[643] Een voorbeeld is de *app* Aipoly[644], die te downloaden is op de smartphone. Door de camera van de smartphone te richten op fysieke objecten herkent het systeem deze objecten. De naam van het object verschijnt in beeld en de naam wordt tevens met een computerstem uitgesproken ten behoeve van bijvoorbeeld blinden en slechtzienden. Een mogelijke toepassing bij het faciliteren van rechtsbescherming zou in de nabije toekomst kunnen zijn dat bij geschillen rond persoonlijke gezondheidsomgevingen, geschillenoplossende software agents 'onderhandelen' met de software agents van de betrokken partijen[645]. Aan andere toepassingen valt ook te denken. In de big-datasamenleving is het bijvoorbeeld voor een individu te complex om zelf na te gaan of de partijen met wie hij de gegevens in zijn persoonlijke gezondheidsomgeving uitwisselt voldoen aan alle voorwaarden die daaraan gesteld zouden moeten worden. Een digitale butler zou gebruikers van een persoonlijke gezondheidsomgeving

640. Al in 1987 introduceerde Apple in een filmpje het idee van een digitale butler. Apple Knowledge Navigator Video (1987), https://www.youtube.com/watch?v=umJsITGzXdo. In 2017 kwam Duursma met het boek 'De Digitale Butler'.
641. In de geest van Selznick 1992.
642. Van Blarkom, Borking, Olk, 2003 p.294 en p.336: "We built JADE applications that use the cryptographic primitives and protocols that are commonly used to implement security and privacy primitives, tested the performance of the overall system in agent environments ranging from one to several thousand agents, and documented all results in terms of timing and processor load." (Documented in deliverable 5.2 van het EU PISA research project).
643. Duursma, 2017.
644. https://www.iphoned.nl/apps/aipoly-vision/.
645. Mulder, Borking, 2006.

kunnen helpen om na te gaan of de andere partij te vertrouwen is, bijvoorbeeld omdat deze bepaalde 'credentials' digitaal kan overleggen.[646]

Bij *privacy-by-design* is het van groot belang dat zichtbaar gemaakt wordt of een toepassing voldoet aan de gestelde wettelijke vereisten. Wat dat betreft kan het in artikel 42 AVG vereiste certificeringsmechanisme gaan helpen om aan te tonen dat aan de voorschriften voor gegevensverwerking door ontwerp- en standaardinstellingen is voldaan. Onder andere via certificering en het transparant bijhouden wat, hoe en waarom persoonsgegevens worden verwerkt kan bovendien worden voldaan aan het verantwoordingsvereiste van de AVG[647]. Certificering is noodzakelijk omdat daar waar *privacy-by-design* in informatiesystemen wordt toegepast, dit zich onttrekt aan de waarneming van het grote publiek.[648] Daarmee krijgen betrokkenen ook meer vertrouwen in het desbetreffende systeem of proces.[649]
De vraag is nog hoe gebruikers kennis kunnen nemen van al dan niet adequate certificering. Certificering van gegevensbescherming is een nieuw fenomeen. Mogelijk kan het bepaalde in artikel 42 AVG over certificering daarbij behulpzaam zijn. Certificering is in de AVG een uitwerking van de aantoonplicht en het transparantievereiste van de AVG. Het is daarom niet meer voldoende dat de verwerkingsverantwoordelijke de gebruikers informeert dat de persoonsgegevens veilig – al dan niet in de *cloud* – zijn opgeslagen. De verwerkingsverantwoordelijke zal moeten aantonen dat de digitale gezondheidsomgeving daadwerkelijk naar de vigerende standaarden veilig is.[650]

7.2.2 MedMij Afsprakenstelsel

Met name in de financiële wereld worden zogenoemde 'afsprakenstelsels' regelmatig toegepast. Bijvoorbeeld door de banken die gezamenlijk iDeal uitbrengen. Ook creditcardmaatschappijen maken afspraken met partijen die in de betaalketen een rol vervullen. Dergelijke afsprakenstelsels kunnen lacunes opvullen op die gebieden waar uitsluitend gebruik van bijvoorbeeld *privacy-by-design* onvoldoende vertrouwen kan geven en wetgeving (nog) niet beschikbaar is. Bij afsprakenstelsels worden relaties met bestaande juridische kaders gelegd.[651] Voor persoonlijke gezondheidsomgevingen is het relevant dat er een publiek-privaat initiatief is van waaruit het Afsprakenstelsel MedMij wordt ontwikkeld.[652]

646. Blarkom van, Borking, Olk, 2003, p. 173 e.v.
647. Zie 6.2.2.
648. Borking 2010 p. 321.
649. Van Rooy en Bus 2009, p.1.
650. Europees kan dit door een audit met een Europees erkend certificaat, zoals bijvoorbeeld op dit moment het Certificaat Van EuroPrise, zie Meissner, 2017. Wat betreft certificering van informatiebeveiliging van gezondheidsgegevens in Nederland kan dit met NEN 7510:2017. Deze nieuwe NEN-norm sinds 1 november 2017 gaat ook over de informatiebeveiliging van gezondheidsgegevens buiten zorgaanbieders. Persoonlijke gezondheidsomgevingen worden daarbij als voorbeeld genomen. Zie verder 6.2.5.
651. De Qiy Foundation (https://www.qiyfoundation.org/), Tippiq (https://www.tippiq.nl/), Kantara initiatief https://kantarainitiative.org/) en anderen werken ieder op hun eigen wijze aan raamwerken op dit vlak. Zie ook het afsprakenstelsel elektronische toegangsdiensten, voorheen eHerkenning: https://afsprakenstelsel.etoegang.nl/.
652. Bij het afsluiten van de tekst voor deze dissertatie was het afsprakenstelsel ontwikkeld tot versie 0.8. Te vinden op https://afsprakenstelsel.medmij.nl/.

MedMij is een initiatief van onder andere patiëntenorganisaties, leveranciers van persoonlijke gezondheidsomgevingen en zorgaanbieders.[653] Het betreft een concept waarbij persoonlijke gezondheidsomgevingen gegevens uit kunnen wisselen met zorgorganisaties. Daartoe is een op vrijwilligheid en zelfregulering gebaseerd afsprakenstelsel in ontwikkeling, dat opgesteld wordt door de deelnemende partijen. MedMij biedt spelregels voor deze uitwisseling. Het betreft juridische, organisatorische, financiële, semantische en technische afspraken. Zo dienen deelnemers aan MedMij bijvoorbeeld te voldoen aan de in subparagraaf 6.2.5 genoemde certificering voor informatiebeveiliging in de zorg via de NEN 7510:2017. Partijen die deelnemen aan het afsprakenstelsel binden zich aan de afspraken en kunnen via het netwerk hun diensten aanbieden.[654]

In het in ontwikkeling zijnde Afsprakenstelsel MedMij worden leveranciers van gezondheidsomgevingen als verwerkingsverantwoordelijken beschouwd. Een persoon kan met behulp van het Afsprakenstelsel MedMij de leverancier van een gezondheidsomgeving erop aanspreken als deze zijn persoonsgegevens niet goed beschermt of meer wil weten over de wijze waarop zijn gegevens worden beschermd. Juist om de zorggebruiker te beschermen, wordt de leverancier van gezondheidsomgevingen in het Afsprakenstelsel MedMij als verwerkingsverantwoordelijke beschouwd en niet de zorggebruiker. Zou de persoon, in de zin van zorggebruiker, verwerkingsverantwoordelijke zijn, dan is er geen enkele partij met plichten jegens hem en heeft de persoon geen rechten ten opzichte van een verwerkingsverantwoordelijke in de zin van de AVG.[655] Overigens heeft de persoon ten opzichte van de verwerkingsverantwoordelijke wel andere privaatrechtelijke rechten om zich op te beroepen, zoals wanprestatie.[656] De persoon is feitelijk niet in staat doel en middelen te bepalen ten opzichte van leveranciers van persoonlijke gezondheidsomgevingen.[657] Deze leveranciers bepalen bijvoorbeeld het informatiebeveiligingsbeleid en daar kan een persoon voor zichzelf geen maatwerk bij vragen, maar er slechts voor kiezen wel of niet mee te doen. De essentie is dat de leverancier van een persoonlijke gezondheidsomgeving juridisch verantwoordelijkheid op zich heeft te nemen. Op deze wijze zijn er jegens de verwerkingsverantwoordelijke leverancier ook sanctionerings- en handhavingsmogelijkheden in het Afsprakenstelsel MedMij en de AVG.

653. Zie www.medmij.nl. 15 november 2017 stond er in Volkskrant een uitgebreid artikel over MedMij:https://www.volkskrant.nl/wetenschap/na-afblazen-landelijk-epd-wordt-aan-vervanger-gewerkt-waarbij-patient-bepaalt-welke-informatie-gedeeld-wordt~a4539159/.
654. De rechtsrelaties en benodigde overeenkomsten voor het afsprakenstelsel MedMij zijn met toelichting te vinden via: https://afsprakenstelsel.medmij.nl/display/PUBLIC/Overeenkomsten+en+rechtsrelaties.
655. De relatie tussen MedMij en de AVG is beschreven in het juridisch kader van MedMij: https://afsprakenstelsel.medmij.nl/display/PUBLIC/Juridisch+kader.
656. Borking, 2012, p.7.
657. Zoals Philips, Apple, Microsoft, maar ook niet ten opzichte van Patient1, Meddex of Pazio.

7.3 RESPONSIEVE GESCHILLENBEHANDELING

7.3.1 Inleiding

In mei 2017 concludeerde het Hague Institute for Innovation of Law (HiiL) op basis van eigen data- en literatuuronderzoek dat in onze rechtsstaat rechters en advocaten voor weinig geld met weinig geschikte middelen verre van optimaal presteren om de problemen van gewone, individuele mensen op te lossen.[658] Een belangrijk probleem is volgens de onderzoekers het 'toernooimodel' waarin de problemen van personen worden gegoten: personen worden tegen elkaar opgezet, waarbij advocaten van beide partijen de claims opdrijven. Het gevolg is dat het conflict scherper kan worden. Soms is dat onvermijdelijk, maar scherp gejuridiseerde conflicten zouden waar mogelijk moeten worden vermeden. In het licht van informationele zelfbeschikking in de zorg is het bijvoorbeeld de vraag in hoeverre bij het gebruik van persoonlijke gezondheidsomgevingen een conflict met leveranciers en zorgaanbieders vermeden kan worden. Personen zoeken volgens HiiL vooral een jurist voor een oplossing, bemiddeling en contact met de andere partij. Volgens de onderzoekers van HiiL moet ons traditionele systeem opnieuw ontworpen worden aan de hand van beschikbare (sociaal) wetenschappelijke kennis.

Er is zowel erkenning voor als kritiek op het onderzoek van HiiL gekomen.[659] Sommigen vonden de toon te somber of te scherp. De ruime publieke aandacht voor dit rapport maakt in ieder geval duidelijk dat er grote behoefte is aan een debat over dit onderwerp.
Evenals Hulst en Van den Bos zie ik het signaal van HiiL als een stimulans voor het denken over en ontwikkelen van meer actieve vormen van probleemoplossing. In de door HiiL voorgestelde procedures hebben partijen een dergelijke meer actieve rol in het oplossen van hun conflict. De aanbevelingen sluiten volgens Hulst en Van den Bos aan bij de al lopende modernisering van rechtspleging en juridische procedures, maar houden geen rekening met enkele rechtspsychologische aspecten. Ten eerste hebben veel juridische conflicten een morele lading, waarbij de gewenste moderniseringsrichting van gezamenlijke probleemoplossing door partijen vaak niet goed of eenvoudig zal werken. Ten tweede stroken de door HiiL voorgestelde moderne en betere procedures niet altijd goed met het realistische perspectief op de redzaamheid van mensen, zoals beschreven in de inleiding van dit hoofdstuk. Een door HiiL voorgestelde actieve probleemoplossende rol in *mediation*-achtige procedures is iets waar mensen waarschijnlijk minder goed voor zijn toegerust wanneer ze minder kennis of opleiding hebben. Het zal juist meer kwetsbare groepen vaker aan cognitieve vermogens ontbreken om het actieve probleemoplossende gedrag te vertonen waarop de voorgestelde procedures ingericht zijn. Daarnaast gaat het bij zelfredzaamheid niet alleen om 'denkvermogen', maar ook om 'doenvermogen.'[660] Ten derde wijzen Hulst en Van den Bos er op basis van eigen empirisch onderzoek op dat heel vaak de

658. HiiL 2017, p.2.
659. Hulst & Van den Bos 2017 en F. Bakker 2017.
660. Zie ook WRR 2017.

overheidsrechter een beslissing moet nemen op een procedureel rechtvaardige manier, zeker in tijden van maatschappelijke polarisatie. Ik ben het met Hulst en Van den Bos eens dat het onderzoek van HiiL ten onrechte de suggestie kan wekken dat de bestaande rechtspraak geëlimineerd zou kunnen worden. Overigens erkent het rapport van HiiL dat de bestaande rechtspraak soms onvermijdelijk zal blijven en dat de rechtspraak in Nederland ondanks de beperkte en gebrekkige middelen van hoge kwaliteit is vergeleken met andere landen.

Het rapport van HiiL geeft inspiratie voor de uitdaging om ook binnen de gezondheidszorg in het licht van de opmars van persoonlijke gezondheidsomgevingen te zoeken naar alternatieve vormen van rechtsbescherming die – conform de theorie van Nonet en Selznick over responsiviteit – aansluiting vinden bij en rekening houden met de praktijk. In feite is *online dispute resolution* (zie verder subparagraaf 7.3.2) een voorbeeld van een dergelijk instrument. HiiL formuleert de volgende aandachtspunten voor instrumenten, zoals online dispute resolution.

Aandachtspunten voor responsieve geschilbeslechting volgens HiiL

1. scherp gejuridiseerde conflicten waar mogelijk vermijden;
2. systeemontwerp aan de hand van beschikbare (sociaal) wetenschappelijke kennis;
3. partijen een meer actieve rol geven in het oplossen van hun conflict.

In de volgende subparagraaf bespreek ik de criteria en uitgangspunten voor *online dispute resolution*.

7.3.2 Online dispute resolution

Online dispute resolution (ODR) wordt al meer dan twintig jaar beschreven in de wetenschappelijke literatuur.[661] Een van de definities die wordt aangehaald is van Ethan Janet Rifkin en Ethan Katsh, waarbij ODR is gedefinieerd als een synergie van *alternative dispute resolution* (ADR) en ICT:

> *"Online Dispute Resolution ('ODR') is dispute resolution that 'takes advantage of the Internet, a resource that extends what we can do, where we can do it, and when we can do it'."*[662]

Bovenstaande definitie is een algemene brede definitie, waaruit te lezen valt dat ODR een aanvulling met behulp van internet is op de bestaande menselijke geschiloplossing.

ODR is gerelateerd aan een breed spectrum van processen, systemen en diensten. Het gemeenschappelijke kenmerk is dat ODR bij alle processen en systemen betrekking heeft op online technologie met als doel om geschillen op te lossen.

661. Legg, 2016,, Condlin 2016, Wing 2016.
662. Katsh and Rifkin, 2001.

Grote big-databedrijven als eBay en Amazon hebben al langer ervaring met hun eigen online geschillenprocedures die werken met slimme algoritmen en zijn gebaseerd op sociaal-wetenschappelijk onderzoek en *big data* over hoe mensen zich gedragen in geschilsituaties. Daarmee kunnen de bedrijven tijd en kosten besparen. Voor personen is het echter niet inzichtelijk op basis van welke algoritmen hun gedrag wordt gestuurd. In die zin hebben personen die bij deze bedrijven diensten afnemen geen informationele zelfbeschikking bij online geschilprocedures.

Alhoewel ODR op dit moment in de gezondheidszorg nog niet beschikbaar is[663], lijkt de toepassing in dit domein ook niet zonder uitdagingen. Bij eBay en Amazon gaat het om relatief eenvoudige vraagstukken, namelijk over de levering van goederen, bijvoorbeeld verkeerd geleverde, kapotte of niet betaalde goederen. Voor persoonlijke gezondheidsomgevingen zullen de vraagstukken wellicht complexer zijn. Toch is het relevant de ontwikkelingen wel in de gaten te houden om te bezien waar wel mogelijkheden zouden kunnen liggen.

Zo is er – buiten de gezondheidszorg – al wel ruime ervaring met ODR, ook in Nederland. Over ODR schreef Verdonschot inzichtelijk in het proefschrift *'Sharing rules that work: Developing law as practical and concrete guidelines for fair sharing'*[664]. Daarbij maakt Verdonschot gebruik van gedragswetenschappelijk onderzoek. Gedragswetenschappelijk onderzoek is ook een belangrijke basis voor de digitale rechtwijzers die onder andere door HiiL zijn ontworpen voor echtscheidingen en burenruzies.[665] Er bestaat nog geen rechtwijzer voor persoonlijke gezondheidsomgevingen, maar dat zou zeker te bepleiten zijn. Bij de ontwikkeling hiervan kan – naast de met echtscheidingen opgedane ervaring aan de hand van *rechtwijzer.nl* – onder andere gebruik worden gemaakt van de ervaring die is in Nederland is opgedaan met E-Court[666], DigiTrage en de Stichting Geschillenoplossing Organisatie & Automatisering (SGOA). Deze termen worden verderop toegelicht. Specifiek voor persoonlijke gezondheidsomgevingen zouden die ervaringen gecombineerd kunnen worden met de afspraken die ontwikkeld worden in het kader van het Afsprakenstelsel MedMij. De geschillenbeslechting bij MedMij is op dit moment nog slechts algemeen geregeld, volgens het klassieke Nederlandse privaatrecht, maar zou in lijn met de online persoonlijke gezondheidsomgevingen – daarnaast – ook via online dispute resolution kunnen.[667]
Gelet op de aandachtspunten van HiiL zou ODR op basis van het Afsprakenstelsel MedMij tot de volgende aandachtspunten leiden:

663. Zie Katsh en Rabinovich-Einy, 2017, hoofdstuk 4 over 'The Internet of On-Demand Healthcare'. De auteurs wijzen op de dringende noodzaak voor ODR en andere online preventieve oplossingen in de gezondheidszorg.
664. Verdonschot, 2013.
665. www.rechtwijzer.nl.
666. Uit onderzoek van het platform voor onderzoeksjournalistiek Investico en Nieuwsuur blijkt dat de rechtspraak zeer kritisch is over dit initiatief. "Niemand weet wat er gebeurt bij e-Court", zegt de voorzitter van de Raad voor de Rechtspraak Bakker. "Ik denk dat het een groot zwart gat is. Je weet niet wie de arbiter is en je weet niet wat hij kan. Eigenlijk heb je geen idee." Zie: https://nos nl/nieuwsuur/artikel/2212374-robotrechter-e-court-is-een-groot-en-niet-transparant-zwart-gat.html.
667. Zie Mulder & Borking, 2006.

1. Scherp gejuridiseerde conflicten waar mogelijk vermijden;
   Vergeleken met het 'toernooimodel' van de rechtszaal zijn scherp gejuridicieerde conflicten al snel te verminderen.
2. Systeemontwerp aan de hand van beschikbare (sociaal) wetenschappelijke kennis;
   De sociaal-wetenschappelijke kennis waar rechtwijzer.nl bij echtscheidingen en burenruzies gebruik van maakt, kan daarbij behulpzaam zijn. Ook de (sociaal) wetenschappelijke onderzoeken die in deze dissertatie aan de orde komen, zoals van CentERData (Universiteit Tilburg), TNO, WRR en SCP kunnen daarbij zinvol zijn.
3. Partijen een meer actieve rol geven in het oplossen van hun conflict;
   Daarbij moet dan wel rekening worden gehouden met het feit dat niet alle gebruikers van persoonlijke gezondheidsomgevingen over het benodigde 'doenvermogen' (WRR 2017) beschikken.

Verder kan praktisch worden geleerd van bestaande Nederlandse ODR-ervaringen, die hieronder kort staan. Allereerst is dat E-Court: een 'internetrechtbank'. Het gaat om hier om private rechtspraak op grond van artikel 1020 e.v. Wetboek van Burgerlijke Rechtsvordering (arbitrage) of artikel 7:900 e.v. BW (bindend advies). De procedures vinden in beginsel online plaats, waarbij zittingen kunnen worden gehouden in het hele land. Een ander voorbeeld is DigiTrage, een stichting die digitale arbitrages voor incassozaken verzorgt. Stichting DigiTrage heeft geen winstoogmerk. Doordat de proceskosten lager zijn dan bij de overheidsrechter, wordt een schuldenaar hier minder mee belast. Het is mogelijk om een DigiTrage-beding op te nemen in de algemene voorwaarden. Betalingsgeschillen die vervolgens ontstaan en niet minnelijk worden opgelost, kunnen worden voorgelegd aan het online scheidsgerecht DigiTrage. De DigiTrage-arbiter wijst na een digitale procedure een arbitraal vonnis. Het vonnis is bindend.

Bekend is SGOA, dat in 1989 is opgericht en waar vanaf 2003 ervaring is opgebouwd met *online mediation*, onafhankelijk van plaats en tijd. De partijen verbinden zich bij SGOA tot een geheimhoudingsplicht. Daarom wordt veel aandacht besteed aan vertrouwelijkheid en beveiliging door het inbouwen van toegangscontroles, wachtwoorden en versleuteling. Met behulp van algoritmen is SGOA in staat om de complexiteit van het voorgelegde geschil snel en eenvoudig te reduceren tot de kern van het probleem. De ervaring bij SGOA leert dat hoe langer een geschil onopgelost blijft, hoe moeilijker het wordt om tot een daadwerkelijke oplossing te komen. Bij offline geschiloplossing blijken wachttijden het grootste obstakel. Bij online geschillenoplossing kan tijd- en plaatsonafhankelijk een geschiloplossing gestart worden. Op internet kunnen – vooral als het straks om vraagstukken over gezondheidsgegevens gaat – de emoties hoog oplopen. Dan is er behoefte aan menselijke tussenkomst. ODR is bij de SGOA daarom niet uitsluitend robotgebaseerd. Indien gewenst kan gebruik gemaakt worden van een menselijke mediator. Overigens blijkt ook uit het empirisch onderzoek van HiiL[668] dat individuen behoefte blijven houden

668. HiiL 2017.

aan een rol voor de menselijke beslisser.[669] Alternatieve of online geschillenbeslechtingstechnieken lijken daarom te moeten inzetten op mechanismen die een combinatie zijn van mens-machine. Dit pleit dus niet voor de genoemde E-Court-dienst, waar primair een robotrechter tot het oordeel komt.

Menselijke geschiloplossers in aanvulling op ODR
Drie typen aanvullende geschiloplossers kunnen in aanvulling op ODR worden overwogen, zeker nu ze ook bij persoonlijke gezondheidsomgevingen een rol kunnen spelen. De typen die hierna worden uitgewerkt zijn: een ombudsfunctie, een informatievertrouwenspersoon en mediators.

Ombudsfunctie
Een ombudsfunctie betreft een onafhankelijke en onpartijdige klachtenbehandeling. Het woord 'ombudsman' komt uit het Zweeds en betekent 'vertegenwoordiger van het volk'. Een ombudsman of iemand anders in een ombudsfunctie vertegenwoordigt een persoon wanneer deze een klacht heeft over de overheid of een organisatie. Hij of zij onderzoekt de klacht en doet daarover een uitspraak.

Veel andere landen hebben dit Zweedse idee aangepast aan hun eigen wensen. Maar in al deze landen staat in de wet dat de ombudsman een onafhankelijke positie heeft. Overigens heeft het woord 'man' in ombudsman niets met het geslacht te maken. Het is afgeleid van het Latijnse woord 'mandataris', wat 'gevolmachtigde' betekent.

Ook in de wereld van internet is een ombudsfunctie denkbaar. Kenmerkend voor een ombudsfunctie zijn een onafhankelijke positie, gezaghebbendheid, eenvoudige toegankelijkheid, laagdrempeligheid onder andere door lage kosten en de snelle wijze waarop de ombudsman een geschil oplost.

Er zijn internationaal al enkele voorbeelden van internetombudsmannen.[670] Op Europees niveau is de Association for Accountability and Internet Democracy (AAID) actief, opgericht door Shefet. Begin 2017 is tijdens een sessie van de Raad van Europa en het Europees Parlement een door AAID voorbereide motie aangenomen met de aanbeveling voor het creëren van een internetombudsman.[671] Dit voorstel werd door 26 parlementariërs en 12 landen omarmd. De voorgestelde ombudsman zal inhoud op internet beoordelen als wettig of onwettig via reviewprocedures.

669. Eerder heeft Ippel (1987 en 2002) al gewezen op het belang van de menselijke maat en persoonlijke inbreng bij klachtenprocedures.
670. Fowlie is de 'Inaugural Ombudsman for the Internet Corporation for Assigned Names and Numbers van ICANN. Frankrijk heeft een Internetombudsman specifiek voor de bescherming van de vrijheid van meningsuiting in voorbereid. Australië heeft al een internetombudsman, deze treedt op als een arbiter en kreeg in 2016 maar liefst 3700 verzoeken voor geschilbeslechting. In België is in 2005 een internetombudsman als particulier gestart met als doel om gedupeerden van eBay en andere veilingplatformen een forum te bieden en groeide uit tot een volwaardige ombudsdienst.
671. Het is nog niet precies duidelijk was de taak van deze internetombudsman wordt. 31 mei 2018 werd door AAID een internationaal congres over dit onderwerp georganiseerd in het Vredespaleis te Den Haag.

Voor persoonlijke gezondheidsomgevingen, bijvoorbeeld via MedMij, kan een ombudsfunctie behulpzaam zijn. Een ombudsfunctie kan voor MedMij behulpzaam zijn, gelet op het belang van onafhankelijkheid, gezag, menselijke maat en persoonlijke inbreng bij klachten en geschillen in het algemeen[672] en in het bijzonder bij de disbalans tussen – soms machtige – leveranciers van persoonlijke gezondheidsomgevingen enerzijds en individuele gebruikers van persoonlijke gezondheidsomgevingen anderzijds. Bovendien gaan de maatschappelijke en technologische ontwikkelingen bij deze applicaties zo snel dat de procedures om toegang en vervolgens een uitspraak te krijgen van de rechter vaak te lang duurt. In de tussentijd zijn er dan al weer vele nieuwe, aangepaste en afgeschafte applicaties zullen zijn. Bovendien is snelle, laagdrempelige toegang en een beoordeling met specifieke kennis van zaken noodzakelijk bij de in opmars zijnde persoonlijke gezondheidsomgevingen.

Informatievertrouwenspersonen
Het idee van een informatievertrouwenspersoon is ontstaan vanuit de ervaring met een patiëntenvertrouwenpersoon (PVP)[673] in de huidige praktijk van de geestelijke gezondheidszorg. Bij een PVP kunnen personen terecht met vragen en klachten over de zorgverlening. Bijvoorbeeld over de manier waarop men met de persoon omgaat bij dwangbehandeling of vrijheidsbeperking.
De PVP is niet in dienst van de zorginstelling waar hij behandeld wordt, maar van de onafhankelijke Stichting PVP en werkt volgens gedragsregels. De PVP behartigt de belangen van de persoon, en doet niets zonder zijn toestemming. De hulp van de PVP is gratis. De PVP ondersteunt alle cliënten die opgenomen zijn, ook als zij minderjarig zijn.

Voor de nog te realiseren informatievertrouwenspersoon zijn dezelfde kenmerken nodig als een ombudsfunctie, aangevuld met meer zorgcontextspecifieke begeleiding, bijvoorbeeld in spanningsvolle situaties in de GGZ. Overigens is voorstelbaar dat een informatievertrouwenspersoon zowel in persoon als online kan functioneren, afhankelijk van de context. Een patiënt in een verzorgingshuis bevindt zich in een andere context dan een patiënt met een blindedarmontsteking en dat is weer anders dan bij psychiatrische patiënten. Bovendien kan hij helpen bij het indienen van een klacht bij de onafhankelijke klachtencommissie.

Het verschil tussen het idee van een ombudsfunctie en een informatievertrouwenspersoon is dat vanuit een ombudsfunctie bijvoorbeeld een rol kan worden gespeeld bij geschillen tussen personen en de leveranciers van hun persoonlijke gezondheidsomgevingen, terwijl informatievertrouwenspersonen met name zullen worden ingezet door zorgaanbieders. Informatievertrouwenspersonen zouden kunnen worden ingezet in verschillende zorgcontexten.

672. Ippel 1987 en 2002.
673. Het concept van de PVP komt uit de geestelijke gezondheidszorg (GGZ). De PVP geeft bij GGZ-instellingen informatie en advies over rechten en plichten bij behandeling bij vragen of klachten waar de persoon met zijn behandelaar(s) niet uitkomt. Daarbij behartigt de PVP de belangen van de persoon en doet niets zonder zijn toestemming. Bovendien is de PVP onafhankelijk, dus niet in dienst van de GGZ maar bij de Landelijke Stichting PVP die gesubsidieerd wordt door VWS.

Mediators
Mediation is – naast rechtspraak en arbitrage – de meest bekende vorm van geschilbeslechting. Er bestaan meerdere opleidingen voor mediators, er is een hoogleraar mediation (VU, rechtsgeleerdheid), er is een tijdschrift voor mediation en rechters verwijzen door naar de mediators die in het register voor mediators staan. Met andere woorden is mediation in Nederland betrekkelijk geïnstitutionaliseerd.

In het register voor mediators zouden wellicht mediators kunnen komen te staan die bijvoorbeeld gaan helpen bij geschillen tussen leveranciers van persoonlijke gezondheidsomgevingen en personen en bij geschillen tussen zorgaanbieders en personen. Te hopen valt dat bijvoorbeeld leveranciers van persoonlijke gezondheidsomgevingen zich responsief opstellen, maar ook dan kunnen er geschillen ontstaan waarbij de leverancier en de betreffende persoon een geschil willen voorleggen aan een mediator.

Inschrijving in het register voor mediators brengt allerlei verplichtingen met zich mee. Er zijn diverse procedurele obstakels denkbaar bij mediation. Hoe zit het bijvoorbeeld met de geheimhoudingsplicht op het moment dat mediation mislukt en een van de partijen alsnog naar de rechter stapt? Mijn inschatting is dat bij gebrek aan wetgeving de rechter de geheimhoudingsplicht van de mediator kan doorbreken met het oog op een 'fair play'.

In Nederland is mediation – in tegenstelling tot in andere landen – nog niet ingebed in wetgeving.[674] In Frankrijk is dit sinds 1995 wel het geval en in de Verenigde Staten bestaat sinds 1998 de *Alternative Dispute Resolution Act*. Mediation via internet in Nederland staat echter niet los van het recht of enige normering. Eerder is het omgekeerde het geval: door het ontbreken van een bestaand juridisch kader is normering des te meer van belang vanwege de rechtszekerheid.[675] Het hiervoor besproken Afsprakenstelsel MedMij voor persoonlijke gezondheidsomgevingen kan hieraan de nodige invulling geven bij toekomstige geschillen tussen leveranciers van persoonlijke gezondheidsomgevingen en personen en bij geschillen tussen zorgaanbieders en personen.

Gegeven de specifieke context van online persoonlijke gezondheidsomgevingen en de aandachtspunten van HiiL kan de inzet van ODR en de geschiloplossers die hiervoor zijn besproken potentieel bijdragen aan verminderde juridicering. Het gebruikmaken van (sociaal) wetenschappelijk onderzoek, mede over de wijze waarop mensen aankijken tegen persoonlijke gezondheidsomgevingen, is vooral van belang bij de ODR-toepassing. Daarbij lijkt de systeeminrichting van de rechtwijzer van rechtwijzer.nl voor echtscheidingen en burenruzies het dichtst in de buurt te komen van de context van persoonlijke gezondheidsomgevingen (meer dan E-Court, DigiTrage en de SGOA). Wat betreft de menselijke geschiloplossers zijn bij persoonlijke gezondheidsomgevingen alle drie de vormen in te zetten, afhankelijk van de situatie. Bij geschillen tussen een verwerkingsverant-

674. Franken, Kaspersen en de Wild, 2004, p.481.
675. Bol 2007.

woordelijke leverancier van persoonlijke gezondheidsomgevingen met een persoon als gebruiker van de betreffende persoonlijke gezondheidsomgeving ligt ODR in combinatie met een ombudsfunctie of een mediator het meest voor de hand. Daarbij is de ombudsfunctie het meest laagdrempelig bij een relatief eenvoudige klacht, terwijl een speciale mediator voor conflicten rond persoonlijke gezondheidsomgevingen meer voor de hand ligt wanneer het gaat om geschil waar beide partijen niet uit komen en samen besluiten dit aan een mediator voor te leggen.
Bij een geschil tussen een gebruiker van een persoonlijke gezondheidsomgeving en een zorgaanbieder ligt een informatievertrouwenspersoon meer voor de hand, vanwege de mogelijk gewenste zorgcontextspecifieke begeleiding. Een patiënt in een verzorgingshuis bevindt zich in een andere context dan een patiënt met een blindedarmontsteking en die context is weer anders bij psychiatrische patiënten. Bovendien kan de informatievertrouwenspersoon helpen bij het indienen van een klacht bij de onafhankelijke klachtencommissie die voor zorgaanbieders bestaat.
Bij alle genoemde vormen hebben de partijen een actieve rol in het oplossen van hun conflict.

7.4 DE RECHTER EN TOEZICHT

7.4.1 Inleiding

Juist omdat bij persoonlijke gezondheidsomgevingen – met een verwerkingsverantwoordelijke van buiten de medische zorg – het medisch beroepsgeheim (zwijgplicht en verschoningsrecht) gedeeltelijk wegvalt[676], is passende rechtsbescherming essentieel. Weliswaar heeft de gebruiker van een persoonlijke gezondheidsomgeving formeel de mogelijkheid om aan de verwerkingsverantwoordelijke toestemming te weigeren om aan derden gegevens te verstrekken, dat betekent niet dat deze gegevens niet alsnog in handen van derden kunnen komen. Een verstrekking aan derden anders dan via toestemming kan rechtmatig zijn als deze derden daartoe over een wettelijke grondslag beschikken (zoals opsporingsinstanties en onder bepaalde omstandigheden, verzekeraars). Ook kan de verstrekking plaatsvinden onder druk (of macht) van partijen zonder dat een rechtmatige grondslag gevonden kan worden. Omdat bij een persoonlijke gezondheidsomgeving, gezondheidsgegevens buiten de medische zorgcontext niet beschermd worden door de zwijgplicht en het verschoningsrecht van de medische hulpverleners, kunnen deze gezondheidsgegevens onder sociale, financiële of wettelijke druk ook inzichtelijk worden voor personen en instanties buiten de gezondheidszorg. Het beroepsgeheim met de zwijgplicht en het verschoningsrecht van medische hulpverleners was voor patiënten de beschermende schil, zowel wettelijk als tuchtrechtelijk. Hoe kan ervoor gezorgd worden dat deze lacune in rechtsbescherming buiten de medische zorgcontext wordt opgevangen?

676. Zie onder andere paragraaf 3.4. over het medisch beroepsgeheim.

In het navolgende wordt rechtsbescherming bij informationele zelfbeschikking binnen en buiten de zorg uitgewerkt vanuit de rol[677] van de rechterlijke macht en de toezichthouders, zoals de AP, de Autoriteit Consument & Markt (ACM) en medische beroepsorganisaties.

7.4.2 De rechter

In voorgaande hoofdstukken is de relevante rechtspraak met betrekking tot informationele zelfbeschikking uiteengezet. Uit die rechtspraak blijkt onder andere dat het recht op informationele zelfbeschikking in Duitsland expliciet wordt erkend. Op het niveau van de EU alsmede in Nederland wordt informationele zelfbeschikking niet als recht erkend, maar wel als een nastrevenswaardig doel voor zover mogelijk. In rechterlijke uitspraken krijgt naast de defensieve informationele zelfbeschikking ook actieve zelfbeschikking steeds meer ruimte.

Een voorwaarde voor een democratische rechtsstaat is dat burgers toegang hebben tot de rechtspraak. Burgers of bedrijven die te maken krijgen met geschillen omtrent persoonlijke gezondheidsomgevingen kunnen zich tot de reguliere rechter wenden als zij niet (meer) kiezen voor een alternatieve vorm van geschillenbeslechting. Op grond van artikel 17 Grondwet en internationale verdragen, zoals het EVRM, kan niemand tegen zijn wil worden afgehouden van de rechten die de wet hem toekent.

Nederlandse rechters worden als onafhankelijk en eerlijk beoordeeld.[678] Ook vindt men de rechter in klantwaarderingsonderzoeken prettig en respectvol. De rechter is de eerste door de Grondwet aangewezen geschilbeslechter. Bij nieuwe, digitale innovatieve toepassingen, zoals persoonlijke gezondheidsomgevingen, zou de verwachting dat de rechter – tijdig – aan de oplossing kan bijdragen lager kunnen liggen, vanwege de indruk dat rechters digitaal op achterstand staan. De mate waarin bij rechters inderdaad de digitale kennis toeneemt, bepaalt de vraag in hoeverre specifieke, in digitale zorg gespecialiseerde rechters nodig zijn, zoals we die inmiddels als wel kennen in de vorm van de Natte kamer (havenzaken), de IE-kamer (octrooizaken) en de Ondernemingskamer. Het research memorandum 'Specialisatie gewenst' van de Raad voor de Rechtspraak sluit naadloos op de trend van specialisatie aan. De hoop wordt daarin uitgesproken dat meer gespecialiseerde rechtspraak zal leiden tot betere uitspraken, snellere procedures doordat uitleg van basiszaken en inschakeling van deskundigen vaak achterwege kan blijven, en meer rechtseenheid. Als mogelijke obstakels worden gezien de vrees dat het duurder (meer rechters) en trager wordt, het uit de pas lopen met rechtsontwikkeling op aanverwante rechtsterreinen en slechtere toegang wanneer gespecialiseerde rechtspraak niet overal

677. Wat betreft het perspectief van de rechtsbescherming ten aanzien van de juridische kwalificering van software voor persoonlijke gezondheidsomgevingen is het Beeldbrigade Arrest (HR, 27 april 2012) van belang. Volgens het Arrest is software noch een roerend goed, noch 'elektriciteit' als zodanig, maar wel een product. Het perspectief van rechtsbescherming ten aanzien van software blijft in deze dissertatie verder buiten beschouwing.

678. Zie ENJC, Independence, Accountability and Quality of the Judiciary Performance Indicators 2017, juni 2017, https://www.encj.eu/images/stories/pdf/GA/Paris/encj_report_ia_2017_adopted_ga.pdf.

beschikbaar is.[679] Sinds 2017 worden gespecialiseerde rechters voor cybercrime overwogen. Deze kunnen mogelijk ook voor de conflicten met betrekking tot het groeiend aantal digitale zorgapplicaties relevant zijn.[680]

7.4.3 Autoriteit Persoonsgegevens

In hoofdstuk 6 kwamen uitspraken van de AP aan de orde. In Nederland is de AP de toezichthouder op de bescherming van persoonsgegevens en daarmee impliciet ook op informationele zelfbeschikking. Tot op heden heeft de AP er prioriteit aan gegeven de verantwoordelijken erop te wijzen dat in strijd wordt gehandeld met de wetgeving ter bescherming van persoonsgegevens en zelfbeschikkingsmogelijkheden van personen. De AP gaf dan de gelegenheid om in overeenstemming met de wetgeving te gaan handelen. Deze werkwijze heeft tot de nodige verbeteringen geleid. Sinds kort is er vanuit de maatschappij en de rechtspraak kritiek gekomen op deze werkwijze.

Recente rechtspraak laat zien dat van de AP meer handhaving en minder gedogen wordt verwacht. Op 7 juli 2017 sprak Rechtbank Utrecht een tussenvonnis uit in een zaak aangespannen door burgerrechtenvereniging Vrijbit dat de AP onvoldoende zou handhaven inzake het DBC-Informatiesysteem (DIS) van de Nederlandse Zorgautoriteit (NZa).[681] De verstrekking van gezondheidsgegevens aan het ministerie van VWS en het CPB was volgens de rechtbank onrechtmatig en de AP zou in actie moeten komen.
In een ander tussenvonnis van de rechtbank van 7 juli 2017, in een zaak eveneens aangespannen door Vrijbit, oordeelt de rechter dat de AP niet juist optreedt inzake de gedragscode van zorgverzekeraars voor het verwerken van gezondheidsgegevens over declaraties.[682] De rechter achtte die code al in 2013 onrechtmatig, maar de AP trad niet handhavend op. De AP had volgens de rechter in deze zaak meer onderzoek moeten doen. Zij had zich niet zonder meer op het standpunt kunnen stellen dat zij geen indicatie had dat de werkwijze van de zorgverzekeraars niet in orde zou zijn. Die indicatie is er namelijk wel: het gegeven dat de zorgverzekeraars nog steeds volgens een gedragscode zouden werken die Rechtbank Amsterdam als onvoldoende heeft beoordeeld. Ook in een kort geding – aangespannen door stichting 'Stop benchmark met ROM' – gericht tegen de verzameling van gepseudonimiseerde GGZ-data voor de Routine Outcome Monitoring (ROM) was er kritiek op het gedoogbeleid van de AP.[683] In deze zaak is de Stichting Benchmark GGZ (SBG) aangewezen als partij om inzicht te geven aan GGZ-instellingen en zorgverzekeraars hoe GGZ-instellingen en -behandelaars presteren. Dit gebeurt op basis van ROM-gegevens die de behandelaars en instellingen zelf verplicht aanleveren aan SBG. Die gegevens komen voort uit vragenlijsten die patiënten invullen over behandeleffecten. De SBG wilde zelf graag dat de AP of een rechter duidelijkheid zou

679. Zie Havinga, Klaassen en Neelis, Raad voor de Rechtspraak 2012.
680. Zie https://dutchitchannel.nl/582115/nederland-denkt-aan-gespecialiseerde-rechters-voor-cybercrime.html.
681. ECLI:NL:RBMNE:2017:3422.
682. ECLI:NL:RBMNE:2017:3421.
683. ECLI:NL:RBMNE:2017:4011.

verschaffen over de vraag of deze ROM-data als persoonsgegevens dienden te worden beschouwd, en of de stichting een wettelijke grondslag had om deze data te mogen benutten in het licht van de veranderde regelgeving en jurisprudentie. Een groep psychiaters, psychologen en patiënten en de Algemene Rekenkamer maakten bezwaar tegen de ROM-methode. Ten eerste dat deze geen bruikbare gegevens oplevert. Ten tweede dat het volgens deze zorgverleners juridisch niet houdbaar is om deze patiëntgegevens zonder toestemming van patiënten aan de stichting over te dragen.

Vanuit de maatschappij, de rechtspraak, de AVG en de UAVG wordt van de AP een pro-actieve en assertieve rol op het terrein van handhaving verwacht. Bijvoorbeeld ten aanzien van de uitbreiding van de rechten van personen (artikel 12-22) en de plichten voor organisaties.[684]

Eerder al stelden Charles Raab en Ivan Szekely[685] op grond van een onderzoek onder *dataprotection authorities* (DPA's), zoals de AP, dat DPA's over onvoldoende kennis en capaciteit beschikken om hun handhavende taak uit te voeren, in het bijzonder gelet op de komende AVG. Raab en Szekely bespreken in hun artikel de resultaten van een enquête onder de DPA's in de EU naar de problemen die zij ervaren bij het begrijpen van en omgaan met nieuwe technologieën. Mede in het licht van de AVG heeft de Tweede Kamer tijdens een beraadslaging over 'Gevolgen Algemene verordening gegevensbescherming voor de AP en meldingen datalekken'[686] aangegeven dat de capaciteit van de AP verdubbeld of verdrievoudigd dient te worden. Dit is tijdens het debat in de Tweede Kamer op 8 maart 2018 over de UAVG nog eens bevestigd. De AP heeft via wijziging van wetsvoorstel UAVG op 9 maart 2018 rechtspersoonlijkheid gekregen en een aanpassing van de begroting. Daarnaast heeft de Tweede Kamer 13 maart 2018 bij het aannemen van het wetsvoorstel UAVG de motie 'hulpvaardige handhaving' aangenomen. De strekking van die motie is dat de AP naast een handhavingstaak, ook een voorlichtingstaak heeft. De AP werd in deze motie AP verzocht in de fase waarin nog veel vragen zijn over de regels, zich primair te richten op voorlichting en hulp bij de interpretatie en uitvoering van de regelgeving, onverlet haar handhavingstaak inzake bewuste schendingen.[687]

Bij de keuze van de Tweede Kamer voor meer menskracht is nog niet de vraag betrokken hoe de AP kan gaan handhaven bij de zelflerende algoritmen in de

684. Zoals het melden van datalekken, *dataprotection by design en default*, functionarissen gegevensbescherming etc.
685. Raab & Szekely 2017.
686. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z07227&did=2017.D15343. Mede op basis van een advies van het adviesbureau Andersson Elffers Felix (AEF), zie: https://www.rijksoverheid.nl/documenten/rapporten/2017/05/31/tk-bijlage-eindrapportage-aef-def. AEF beschrijft in zijn rapport drie scenario's (laag-midden-hoog) voor verwachte werkstromen. Per scenario heeft AEF het benodigde aantal fte's en financiële middelen berekend waarmee de AP op een efficiënte en effectieve wijze invulling kan geven aan haar (nieuwe) taken en bevoegdheden. Het berekende aantal fte's varieert van minimaal 185 tot maximaal 270 fte's. Dit betekent een groei van bijna 2 tot 3 keer ten opzichte van de formatie in 2017.
687. Zie: https://zoek.officielebekendmakingen.nl/dossier/34851/kst-34851-18?resultIndex=10&sorttype=1&sortorder=4.

big-datasamenleving.[688] Een bijkomstigheid van *big data* is dat personen en toezichthouders vaak helemaal niet weten dat hun data worden verwerkt, wat handhaven lastig maakt.
Wellicht dat de AP ook algoritmisten aan zal moeten gaan nemen. Zou de *black box* met zelflerende algoritmen in het bezit van 'grootdatabezitters' – zowel bedrijven als overheden – te openen moeten zijn via (verplichte) audits door onafhankelijke toezichthouders, zoals de AP of de ACM? Deze verplichte audits door onafhankelijke toezichthouders zouden dan bijvoorbeeld op een vergelijkbare wijze kunnen worden vormgegeven als nu in jaarrekeningenrecht. Zoals accountants financiële stromen controleren, zo is voorstelbaar dat toezichthouders voor de gegevensbescherming dat voor persoonsgegevensstromen zouden kunnen doen. Het is in het belang van personen dat van de bescherming van persoonsgegevens een 'plicht' wordt gemaakt voor organisaties die met *big data* werken. Organisaties die met *big data* werken zijn overheden en het groeiende aantal bedrijven dat grote hoeveelheden data analyseert.[689]Wat betreft bedrijven – en daarmee ook leveranciers van persoonlijke gezondheidsomgevingen – is het consumentenbeschermingsrecht van belang. De ACM ziet toe op de naleving van deze regels[690].

7.4.4 Autoriteit Consument & Markt

Gelet op de beperkte capaciteit van de ACM en het – ook voor persoonlijke gezondheidsomgevingen – toenemende belang van consumentenrechtenbescherming en de zeker ook beperkte kennis en deskundigheid op het specifieke terrein van het mededingingsrecht bij de AP dienen de toezichthouder op het mededingingsrecht, de ACM[691]en de AP effectief met elkaar samen te werken en taken en bevoegdheden op elkaar af te stemmen. De bevoegdheid van ACM tot handhaving van consumentenrechten is beperkt tot inbreuken met een 'collectief karakter'. Het mededingingsrecht heeft tot doel marktmacht te beteugelen en de vrije concurrentie te beschermen in het belang van de consument. De Duitse mededingingsautoriteit – *Bundeskartellamt* – heeft bijvoorbeeld, net als diverse andere (nationale) toezichthouders al eerder deden en op dit moment doen, in maart 2016 een onderzoek gedaan naar mogelijk machtsmisbruik bij Facebook.[692] In dit onderzoek staan de algemene gebruiksvoorwaarden voor persoonlijke data centraal. Facebook zou haar machtspositie misbruiken door onduidelijke voorwaarden te hanteren, waardoor haar gebruikers geen

688. Zie bijvoorbeeld Harari (2016).
689. Van der Sloot (2017).
690. Zie Moerel & Prins 2016, zij verwijzen in voetnoot 285 naar de minister van Economische Zaken: "Ook mag niet op een oneerlijke manier gebruik worden gemaakt van het begrip «gratis» of bewoordingen van gelijke strekking. Hiervan zou sprake kunnen zijn als apps of diensten als gratis worden geadverteerd terwijl in wezen sprake is van een uitruil doordat de gegevens van de consument worden uitgelezen. Ook moet de aanbieder van een digitale dienst de consument informeren of de digitale inhoud wordt gebruikt voor het in kaart brengen van consumentengedrag (ook wel bekend als tracking). Kamerstukken II, 2014/15, 32761, nr. 78, p. 4.
691. Voor zover persoonlijke gezondheidsomgevingen worden aangeboden door zorgaanbieders kan ook de toezichthouder op de 'zorgmarkt', de NZa, van belang zijn. AP en NZa werken ook al samen.
692. Oktober 2017 is ook in de rechtbank van Brussel de juridische strijd begonnen tussen Facebook en de Belgische Privacycommissie.

overzicht of controle hebben over de data die zij delen, met andere woorden: geen informationele zelfbeschikking hebben. Facebook vergroot haar machtspositie door Facebookgebruikers aan te sporen meer persoonlijke informatie te delen via de Facebookapp en de Facebookmessengerapp. De Duitse toezichthouder meent dat Facebook zich niet houdt aan de speciale verantwoordelijkheden die marktpartijen met een dominante marktpositie volgens de rechtspraak over misbruik van machtspositie hebben.[693]

Het mededingingsrecht kan ten dienste staan van privacy, gegevensbescherming en informationele zelfbeschikking. Dat kan door hulp van de mededingingsautoriteit aan de AP , maar wellicht is het effectiever door een goede taak- en bevoegdheidsverdeling en waar nodig samenwerking af te spreken tussen de mededingings- en de gegevensbeschermingsautoriteit. Handhaving van privacy en gegevensbescherming in Europa vindt tot nu toe nog vrijwel uitsluitend plaats door nationale toezichthouders voor privacy- en gegevensbescherming.[694] Kannekens & Van Eijk bepleiten een meer marktconsumenten gerelateerde benadering. Foutief gedrag in de context van privacy en het verwerken van persoonsgegevens is volgens hen vooral ingegeven door economische overwegingen en niet door een streven om een fundamenteel recht te schenden. Het tweede volgt meer uit het eerste. Fundamentele rechten zijn zo waardevol dat daaraan – anders dan aan oneerlijke handelspraktijken – geen prijskaartje kan worden gehangen. Dit moet volgens hen consequenties hebben voor de naleving en handhaving: die dient in de eerste plaats consumentgericht te zijn. Privacyvraagstukken met een kleine 'p' – waar het dus vooral om marktgedrag gaat – horen volgens Kannekens & Van Eijk primair binnen de marktregulering te worden opgelost. Daar past dus bij dat Europese markt en consumententoezichthouders zich actiever opstellen, al dan niet in afstemming met privacytoezichthouders. Het is immers hun taak voor de markt en consumentenbelangen op te komen. Het is effectiever direct sancties op te kunnen leggen, zonder dat eerst een aanwijzing noodzakelijk is van de AP. Effectieve handhaving dient tevens gericht te zijn op preventie en gedragsverandering. Met Kannekens & Van Eijk ben ik van mening dat artikel 49a Mededingingswet – waarin de bevoegdheid is geregeld om een toezegging bindend te verklaren – een mogelijke basis kan zijn om te komen tot een gedragsveranderende maatregel.

In de context van *big data* liggen persoonsgegevens ten grondslag aan het verdienmodel van grote platforms. Ook de Europese toezichthouder voor gegevensbescherming is van mening dat de handhaving via het mededingingsrecht een effectieve manier is om bij te dragen aan een betere databescherming.[695]

693. Zie Gerecht 1 juli 2010, T-231/05, AstraZeneca/Commissie, ECLI:EU:T:2010:266, punt 355.
694. Kannekens & Van Eijk (2016).
695. Preadvies van de Europese toezichthouder voor gegevensbescherming, Privacy and competiteveness in the age of big data: The interplay between dataprotection, competition law and consumer protection in the Digital Economy. maart 2014, p.26.

7.4.5 Inspectie Gezondheidszorg en Jeugd

In hoofdstuk 6 kwam het toezicht van de IGJ al aan de orde. Net als bij de ACM is het van belang de taken en bevoegdheden goed af te stemmen in de samenwerking met de AP bij het toezicht op persoonlijke gezondheidsomgevingen. Persoonlijke gezondheidsomgevingen kunnen medische hulpmiddelen zijn als zij een diagnostische of therapeutische functionaliteit hebben. Diverse van de 350.000 gezondheidsapps hebben een diagnostische of therapeutische functionaliteit en kunnen geïntegreerd worden met een persoonlijke gezondheidsomgeving. Daarmee vallen vele persoonlijke gezondheidsomgevingen nu of in de nabije toekomst naast het toezicht van de AP ook onder het toezicht van de IGZ. Een effectieve verdeling van de taken en bevoegdheden van de betreffende toezichthouders is daarbij van belang gelet op de beperkt beschikbare capaciteit.

7.5 CONCLUSIE

In dit hoofdstuk stonden de derde en vierde onderzoeksvraag centraal in het licht van rechtsbescherming in ruime zin.

Wat betreft de derde onderzoeksvraag bleek dat normering ook gestalte kan krijgen in de applicaties zelf via *privacy-by-design*. Bij het faciliteren van persoonlijke gezondheidsomgevingen met behulp van *privacy-by-design* kan dit betekenen dat personen die dit kunnen of willen, op elk gewenst moment toegang krijgen tot hun gezondheidsgegevens. Daarnaast kunnen met behulp van speciale digitale butlers voor persoonlijke gezondheidsomgevingen personen worden beschermd in de complexe big-datasamenleving. In de algoritmen van de digitale butler kunnen bovendien per persoon en per context specifieke voorwaarden en voorkeuren worden opgenomen. Om dit mogelijk te maken zal de digitale butler op deze wijze ontwikkeld dienen te worden. Bovendien dient onderzocht te worden of de investeringen opwegen tegenover het te verwachten gebruik door personen. Verder is het raadzaam rechtsbescherming te bieden door als default setting te eisen dat smartphones standaard geen signalen afstaan aan de buitenwereld.

Wat betreft de vierde onderzoeksvraag zijn met het oog op toekomstige ontwikkelingen, gelet op de opmars van persoonlijke gezondheidsomgevingen, de navolgende aanbevelingen gedaan ten behoeve van meer informationele zelfbeschikking.

De eerste aanbeveling is dat het in ontwikkeling zijnde Afsprakenstelsel MedMij, waar mogelijk, wordt ingezet voor informationele zelfbeschikking, zodat iedereen die dat wil online zijn eigen gezondheidsgegevens kan verzamelen en gebruiken.
Bovendien dient het Afsprakenstelsel MedMij de persoon ten opzichte van de leverancier van persoonlijke gezondheidsomgevingen en de samenleving te beschermen tegen misbruik van gegevens. De crux is dat de aanbieder van de persoonlijke gezondheidsomgeving juridisch verwerkingsverantwoordelijk is.

De tweede aanbeveling is dat ODR op vrijwillige en vrijblijvende basis de keuze biedt om (al dan niet algoritme-gestuurd) bij te dragen aan de mate waarin kwetsbare personen worden beschermd. De mate waarin mensen worden beschermd dan wel bedreigd, hangt af van de werking van algoritmen in de digitale procedures. Van belang daarbij is ook in hoeverre dit transparant en controleerbaar is voor de betrokken persoon. Zelflerende algoritmen zijn niet te doorzien voor de gemiddelde burger. ODR kan gebruikmaken van algoritmen die gebaseerd zijn op kennis uit de praktijk met behulp van de gedragswetenschappen, waardoor de snelheid en toegankelijkheid van rechtsbescherming wellicht verbeterd worden. Via ODR kan rekening worden gehouden met verschillende zorgcontexten. Afhankelijk van de zorgcontext is er behoefte aan verschillende menselijke, onafhankelijke geschiloplossers. Bij een geschil tussen een persoon en een leverancier van een persoonlijke gezondheidsomgeving, geleverd door een bedrijf buiten de zorgcontext, kan een internetombudsman behulpzaam zijn. Bij een geschil tussen een persoon en een patiëntenportaal van een zorgaanbieder kan juist een informatievertrouwenspersoon geschikter zijn. Afhankelijk van het type zorg, zoals psychiatrie, fysiotherapie of maatschappelijk werk, kan er behoefte zijn aan verschillende soorten informatievertrouwenspersonen. Bovendien is contextspecifieke begeleiding mogelijk, bijvoorbeeld in spanningsvolle situaties in de GGZ. Een register met mediators specifiek voor persoonlijke gezondheidsomgevingen biedt optimale mogelijkheden om rekening te houden met de context.

De derde aanbeveling is dat alternatieve of online geschillenbeslechtingstechnieken worden aangevuld met menselijke geschiloplossers – zoals een ombudsfunctie, een informatievertrouwenspersoon of een mediator – die kunnen bijdragen aan ruimte voor emoties en het bieden van vertrouwen, zodat wordt voorkomen dat het proces ‘robotachtig’ wordt.

Tot besluit zijn er aanbevelingen gedaan voor het wettelijk regelen van het ‘patiëntgeheim’ en de bijbehorende zwijgplicht en het verschoningsrecht en het verbod op het commercieel exploiteren van gezondheidsgegevens.

8. *Conclusies en aanbevelingen*

8.1 INLEIDING

Een eerste conclusie die aan de hand van de eerdere hoofdstukken getrokken kan worden, is dat het concept van 'informationele zelfbeschikking' in de rechtspraak en in juridische publicaties is ontwikkeld en door de introductie en massale verspreiding van mobiele gegevensdragers inmiddels een andere strekking krijgt. Informationele zelfbeschikking was eerst vooral een defensief 'instrument' om de eigen persoonlijke levenssfeer te beschermen en af te schermen tegen derden. Nu krijgt het begrip een 'positieve', 'actieve' lading doordat personen de keuzevrijheid en ontplooiingsmogelijkheden krijgen om zelf te beslissen over wat er met hun persoonsgegevens gebeurt en deze ook zelf te (laten) beheren. Bovendien geeft nieuwe wet- en regelgeving in de Algemene verordening gegevensbescherming (AVG), de Uitvoeringswet AVG en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabpvz) aan personen steeds meer informationele zelfbeschikkingsrechten, zoals elektronische inzage, (gespecificeerde) toestemming en dataportabiliteit voor zover het gaat om gegevens die door de betrokkene zelf zijn verstrekt.

De tweede conclusie is dat relevante maatschappelijke en technologische ontwikkelingen, zoals de opkomst van persoonlijke gezondheidsomgevingen via mobiele gegevensdragers en het gebruik van big-dataprofilering met behulp van kunstmatige intelligentie , leiden tot een systematische disbalans tussen de machtscapaciteit van bedrijven en overheden enerzijds, en die van personen anderzijds.

Tegen deze achtergrond zijn in dit proefschrift de volgende onderzoeksvragen onderzocht:

I Wat dient, mede in het licht van technologische ontwikkelingen, te worden verstaan onder informationele zelfbeschikking? Is informationele zelfbeschikking mogelijk en wenselijk, in hoeverre en met welke beperkingen? Kan en moet daarbij onderscheid worden gemaakt naar typen personen?
II Wat betekent een en ander concreet voor de – ook historisch gegroeide en ontwikkelde – uitwerking van informationele zelfbeschikking via regulering?
III Normering kan ook gestalte krijgen in de applicaties zelf, namelijk via *privacy-by-design.* Deze en andere mogelijkheden kunnen in potentie personen faciliteren bij het beheer van hun gezondheidsgegevens. Maar wat betekent dit concreet op het terrein van gezondheid en gezondheidszorg?

IV Welke overige toekomstgerichte aanbevelingen zijn er – gelet op de opmars van persoonlijke gezondheidsomgevingen – te geven om informationele zelfbeschikking te realiseren?

8.2 MOGELIJK, WENSELIJK EN TYPE PERSONEN

Ad 1) Wat dient, mede in het licht van technologische ontwikkelingen, te worden verstaan onder informationele zelfbeschikking? Is informationele zelfbeschikking mogelijk en wenselijk, in hoeverre en met welke beperkingen? Kan en moet daarbij onderscheid worden gemaakt naar typen personen?

Wat dient, mede in het licht van technologische ontwikkelingen, te worden verstaan onder informationele zelfbeschikking?
Informationele zelfbeschikking is gedefinieerd als het vermogen van een persoon om in beginsel zelf te bepalen in hoeverre persoonsgegevens worden gebruikt en verder bekendgemaakt, met het oog op een zelfbepaald leven. De mate waarin personen daadwerkelijk het vermogen hebben om zelf te bepalen in hoeverre persoonsgegevens over hen worden gebruikt, wordt beïnvloed door:

- de opkomst van persoonlijke gezondheidsomgevingen via mobiele gegevensdragers en
- het gebruik van big-dataprofilering met behulp van kunstmatige intelligentie door bedrijven en overheden.

De technologische ontwikkelingen leiden tot een systematische disbalans tussen de machtscapaciteit van bedrijven en overheden om over persoonsgegevens te beschikken enerzijds, en die van de betrokken personen anderzijds.

Is informationele zelfbeschikking mogelijk?
Uit de beschreven praktijkontwikkelingen in tweede hoofdstuk blijkt dat er sprake is van een explosief aanbod van technologie, dat mogelijkheden lijkt te scheppen om 'informationele zelfbeschikking' actiever en assertiever vorm te geven. De behoefte en mogelijkheden om gebruik te maken van persoonlijke gezondheidsomgevingen nemen toe. Hoewel deze ontwikkeling nog in de kinderschoenen staat, kan het snel gaan. Zoals ook de opkomst van de smartphones snel is gegaan. Het enorme commerciële succes van de smartphone heeft de persoonlijke gezondheidsomgeving letterlijk binnen handbereik gebracht. Er bestaan reeds vele apps die het bijhouden en beïnvloeden van de eigen gezondheid mogelijk maken.
Aan de hand van de beschreven praktijkontwikkelingen in het tweede hoofdstuk blijkt dat voor personen informationele zelfbeschikking in absolute zin – waarbij personen echt volledige keuzevrijheid hebben en weten waarvoor zij kiezen en toestemming geven – een illusie is Door big-dataprofilering, ondoorzichtige algoritmen en complexe, onzichtbare online datahandel ontstaat een systematische disbalans tussen de machtscapaciteit van bedrijven en overheden enerzijds, en die van personen anderzijds.

Uit het aangehaalde onderzoek blijkt eveneens dat personen begeleiding en hulp nodig hebben van hulpverleners, familieleden en vrienden bij het uitoefenen van informationele zelfbeschikking, met name in spanningsvolle situaties rond (ernstige) diagnoses en bij mensen die niet goed in staat zijn over zichzelf te beschikken. Ook in de geneeskundige literatuur wordt shared decision making vaak gezien als een stap op weg richting meer zelfbeschikking voor de patiënt en een evenwichtigere zorgverlener-patiëntrelatie. Al het aangehaalde onderzoek en de bijbehorende literatuur gaat niet uit van een ideaal van volledige informationele zelfbeschikking in de zorg, maar van een verandering in de rol van zorgverleners naar die van begeleider van personen of van andere een helpende hand van een mens of machine, zoals een digitale butler.
Juist bij ingewikkelde geneeskundige behandelingen zal er sprake zijn van een samenspel tussen zorgverlener en patiënt. Zorgverleners zullen zich naar verwachting meer gaan toeleggen op complexe diagnostiek en gezamenlijke besluitvorming, waarin persoonlijke afwegingen belangrijk zijn.
Informationele zelfbeschikking in relatieve, impliciete zin lijkt in beginsel wel steeds meer mogelijk voor personen die dit kunnen of willen via persoonlijke gezondheidsomgevingen en patiëntenportalen van zorgaanbieders.
Uit de rechtspraak is gebleken dat het recht op informationele zelfbeschikking in Duitsland weliswaar expliciet wordt erkend, maar tevens onvoldoende rechtsbescherming biedt tegen de snelle maatschappelijke en (informatie)technologische ontwikkelingen. Vandaar dat in Duitsland het 'computer-grondrecht' is geformuleerd dat beoogt bescherming te bieden tegen het gebruik van informatiesystemen.
Op het niveau van de EU alsmede in Nederland wordt informationele zelfbeschikking niet als recht erkend, maar wel als een nastrevenswaardig doel voor zover mogelijk. In rechterlijke uitspraken krijgt naast de defensieve informationele zelfbeschikking ook actieve zelfbeschikking steeds meer ruimte. Al met kan worden geconcludeerd dat informationele zelfbeschikking in de zorg gelet op maatschappelijke, technologische en juridische ontwikkelingen in absolute zin een illusie is, maar in relatieve, impliciete zin steeds meer en beter mogelijk wordt. Zowel in de praktijk door de opmars van persoonlijke gezondheidsomgevingen en smartphones, als in het recht door steeds meer actieve informationele zelfbeschikkingsrechten en jurisprudentie.

Is informationele zelfbeschikking wenselijk?
Informationele zelfbeschikking is onderzocht in Duitsland, Europa en Nederland. Als eerste is gekeken naar Duitsland, de bakermat voor informationele zelfbeschikking. Voor Duitsland kan worden geconcludeerd dat het recht op informationele zelfbeschikking in beginsel wenselijk is binnen het Duitse rechtsstelsel. Informationele zelfbeschikking is in Duitsland een facet van het algemeen persoonlijkheidsrecht en het recht op menselijke waardigheid. Het recht op informationele zelfbeschikking blijkt in Duitsland onvoldoende rechtsbescherming te bieden tegen het gebruik van informatiesystemen. Vandaar dat het Hof het 'computer-grondrecht' heeft geformuleerd dat beoogt bescherming te bieden tegen het gebruik van informatiesystemen.

In het Europese en Nederlandse recht is er geen expliciet recht op informationele zelfbeschikking, wel impliciet. Er is Europese en Nederlandse wetgeving ter bescherming van persoonsgegevens, zoals de AVG, op grond waarvan verwerkingsverantwoordelijke bedrijven en overheden plichten hebben en personen rechten. In de Nederlandse wetgeving zijn er aanvullende informationele zelfbeschikkingsrechten voor personen ten opzichte van zorgaanbieders, maar geen aanvullende rechten ten opzichte van verwerkingsverantwoordelijke bedrijven en overheden die gezondheidsgegevens verwerken via persoonlijke gezondheidsomgevingen. Aanvullende rechtsbescherming is wenselijk ten behoeve van meer informationele zelfbeschikking.

Typen personen
De groepen personen die in de discussie over informationele zelfbeschikking juridische en morele aandacht nodig hebben zijn:

– personen die zich zorgen maken over machtsmisbruik;
– personen die gegevens niet kunnen of willen 'managen' en
– personen die actief zelf persoonsgegevens willen 'managen'.

Deze drie te onderscheiden groepen sluiten aan op de drie verschillende discoursen van patiëntgerichte in de dissertatie van Pluut.

8.3 REGULERING

Ad 2) Wat betekent het een en ander concreet voor de – ook historisch gegroeide en ontwikkelde – uitwerking van informationele zelfbeschikking via regulering?

In Europa en Nederland blijkt er – anders dan in Duitsland – geen algemeen recht op informationele zelfbeschikking te bestaan. In het Handvest met de Europese grondrechten vormen het recht op privéleven en het recht op gegevensbescherming twee afzonderlijke grondrechten. In Europa en Nederland is naast het recht op privéleven voor de informatiesamenleving het concept 'bescherming van persoonsgegevens' ontwikkeld. Wel bestaan er op dit moment – binnen de Nederlandse zorgcontext – actieve, afzonderlijke, 'informationele zelfbeschikkingsrechten', die met name te vinden zijn in de Wet geneeskundige behandelingsovereenkomst (artikel 7:446 e.v. BW) en in het bijzonder in de Wabvpz. Informationele zelfbeschikking blijkt zich binnen de Nederlandse zorg zowel in de regulering als de rechtspraak van 'negatieve' afweerrechten naar 'positieve' participatierechten te ontwikkelen.

In de AVG zijn eveneens afzonderlijke 'informationele zelfbeschikkingsrechten' ondergebracht. Voor persoonlijke gezondheidsomgevingen is onder andere het recht op dataportabiliteit van belang. Dit nieuwe recht is nauw verbonden met het recht op inzage, maar verschilt hier ook van. Het recht op dataportabiliteit betreft de overdraagbaarheid van gegevens. Het houdt in dat de persoon het recht heeft de persoonsgegevens die hij aan een verantwoordelijke heeft verstrekt in een gestructureerde, gangbare en machineleesbare vorm te ontvangen,

zodat hij deze aan een andere verantwoordelijke kan overdragen. Het doel van dit nieuwe recht is de positie van personen te versterken en hun meer controle over hun gegevens te geven. Voor persoonlijke gezondheidsomgevingen is het recht op dataportabiliteit van toepassing voor zover gegevens in een medisch dossier of persoonlijke gezondheidsomgeving door de betrokkene zelf zijn verstrekt aan de zorgaanbieder of de leverancier van een persoonlijke gezondheidsomgeving. Dit recht is – ten dele – een stimulans voor het tot stand komen van persoonlijke gezondheidsomgevingen, omdat het succes hiervan staat of valt met de mogelijkheid om gegevens over te dragen. Bij een recht op dataportabiliteit voor alle gegevens in een medisch dossier of persoonlijke gezondheidsomgeving van de betrokkene zou de ontwikkeling van persoonlijke gezondheidsomgevingen nog meer bijdragen aan informationele zelfbeschikking. Het gaat om een nieuw recht waar nog ervaring mee moet worden opgedaan. Mocht in de praktijk blijken dit nieuwe recht – door de beperking dat het alleen om tot door de betrokkene zelf verstrekte gegevens gaat – de ontwikkeling van informationele zelfbeschikking via persoonlijke gezondheidsomgevingen teveel belemmeren, dan valt wetgeving te overwegen om de reikwijdte van artikel 20 AVG te verruimen. Aan de andere kant kan het recht op dataportabiliteit er ook toe leiden dat andere (ook kwaadwillende) partijen eenvoudiger de beschikking kunnen krijgen over de gezondheidsgegevens in de persoonlijke gezondheidsomgevingen. Aanvullende juridische, organisatorische en technologische maatregelen om gezondheidsgegevens – met name buiten de zorgcontext – te beschermen zijn door het (gedeeltelijke) recht op dataportabiliteit daarmee extra van belang. In die zin biedt de AVG ook zelf al waarborgen tegen kwaadwillenden, maar houdt de technologie neutrale AVG niet specifiek rekening met persoonlijke gezondheidsomgevingen.

Wat betreft wetgeving wordt niet of nauwelijks geanticipeerd op de komst van persoonlijke gezondheidsomgevingen. Bij die omgevingen zal er sprake zijn van verwerkingsverantwoordelijken die doorgaans van buiten de zorg komen. Er wordt van de zijde van de wetgever nog niet geanticipeerd op de toenemende invloed van private aanbieders van persoonlijke gezondheidsomgevingen. Deze toenemende invloed van private aanbieders heeft risico's op misbruik als mogelijk gevolg.

Op basis van de analyse in deze dissertatie is mijn stelling dat de geschetste ontwikkelingen, die bedrijven en overheden een grotere machtscapaciteit over gezondheidsgegevens geeft, een vorm van tegenmacht behoeft. Daarbij biedt het medisch beroepsgeheim – dat van oudsher voor medische dossiers geldt – vrijwel geen rechtsbescherming meer. Er is kortom behoefte aan aanvullende regulering om personen actief te beschermen. Aanvullende regulering zou bijvoorbeeld vorm kunnen krijgen via een zwijgplicht en verschoningsrecht voor verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen in een nog te formuleren wetgeving. Deze wetgeving zou rekening moeten houden met het feit dat gezondheidsgegevens in belangrijke mate verwerkt worden door verwerkingsverantwoordelijken van buiten de zorg. Deze nog te formuleren wetgeving zou net als de Wabvpz aanvullend kunnen zijn op de AVG, met bijbehorende internationale werking.

8.4 NORMERING IN APPLICATIES

Ad 3) Normering kan ook gestalte krijgen in de applicaties zelf, namelijk via *privacy-by-design*. Deze en andere mogelijkheden kunnen in potentie personen faciliteren bij het beheer van hun gezondheidsgegevens. Maar wat betekent dit concreet op het terrein van gezondheid en gezondheidszorg?

Wat betreft de derde onderzoeksvraag bleek dat normering ook gestalte kan krijgen in de applicaties zelf, via *privacy-by-design*. Bij het faciliteren van persoonlijke gezondheidsomgevingen betekent dit concreet dat personen de keuzevrijheid kunnen krijgen om op elk gewenst moment *real time* toegang te krijgen tot hun gezondheidsgegevens. Daarnaast kan een speciale digitale butler personen beschermen in de complexe big-datasamenleving. In de algoritmen van de digitale butler kunnen per persoon en per context specifieke voorwaarden en voorkeuren worden opgenomen.

8.5 AANBEVELINGEN TOEKOMSTIGE ONTWIKKELINGEN

Ad 4) Welke overige toekomstgerichte aanbevelingen zijn er – gelet op de opmars van persoonlijke gezondheidsomgevingen – te geven om informationele zelfbeschikking te realiseren?

1. Afsprakenstelsel MedMij
Het in ontwikkeling zijnde Nederlandse Afsprakenstelsel MedMij – afkomstig uit de praktijk van zorggebruikers, zorgaanbieders en leveranciers van persoonlijke gezondheidsomgevingen, gestimuleerd door de overheid en zorgverzekeraars – dient bij te dragen aan informationele zelfbeschikking voor de gebruikers van de persoonlijke gezondheidsomgevingen.

Bovendien moet in het Afsprakenstelsel MedMij de persoon ten opzichte van de leverancier van persoonlijke gezondheidsomgevingen en de samenleving worden beschermd door te benadrukken dat de persoon geen verwerkingsverantwoordelijke is in de zin van de AVG. De crux is dat de aanbieder van de persoonlijke gezondheidsomgeving juridisch een verwerkingsverantwoordelijke is met plichten en de persoon, als gebruiker, met rechten. Als blijkt dat het Afsprakenstelsel MedMij onvoldoende rechtsbescherming biedt, dienen de toezichthouders in te grijpen. Daarbij is een effectieve taakverdeling tussen de toezichthouders aan te bevelen. Indien MedMij onvoldoende rechtsbescherming blijkt te bieden, lijkt op dat moment aanvullende wet- en regelgeving aan de orde. Aan het einde van deze paragraaf volgen nog twee aanbevelingen die vanuit het perspectief van toekomstige regulering in dit verband van belang zijn.

2. Online geschillenbeslechting
Gegeven de specifieke context van online persoonlijke gezondheidsomgevingen beveel ik verschillende vormen van *online dispute resolution* (ODR) met menselijke geschiloplossers aan. Dit mede ter voorkoming van juridicering. Bij persoonlijke

gezondheidsomgevingen zijn voor verschillende typen van geschillen onderscheidende vormen van menselijke geschiloplossers in te zetten. Ten eerste is dit mogelijk bij geschillen tussen een verwerkingsverantwoordelijke leverancier van persoonlijke gezondheidsomgevingen en een persoon als gebruiker van de betreffende persoonlijke gezondheidsomgeving. In dat geval ligt ODR in combinatie met een ombudsfunctie of een mediator het meest voor de hand. Een ombudsfunctie is het meest laagdrempelig in het geval van een relatief eenvoudige klacht. Een speciale mediator voor conflicten rond persoonlijke gezondheidsomgevingen ligt meer voor de hand indien beide partijen er niet uitkomen en samen besluiten dit aan een mediator voor te leggen.
Ten tweede ligt bij geschillen tussen de gebruiker van een persoonlijke gezondheidsomgeving en zorgaanbieders een informatievertrouwenspersoon meer voor de hand, vanwege de mogelijk gewenste zorgcontextspecifieke begeleiding. Bovendien kan een informatievertrouwenspersoon helpen bij het indienen van een klacht bij de onafhankelijke klachtencommissie die voor zorgaanbieders bestaat. Bij alle genoemde vormen hebben de partijen een actieve rol in het oplossen van hun conflict.

3. Kennisbasis binnen rechtspraak aangaande digitalisering.
Voor situaties waarbij sprake is van toegang tot de rechter en toezichthouders is juist bij persoonlijke gezondheidsomgevingen – vaak met verwerkingsverantwoordelijken van buiten de medische zorg – passende rechtsbescherming noodzakelijk. De ontwikkeling van digitale persoonlijke gezondheidsomgevingen alsmede het type gegevens dat hierbij word gebruikt en de mogelijk kwetsbare positie van gebruikers van dergelijke omgevingen, toont het belang van een goede kennisbasis binnen de rechtspraak aangaande de kenmerken en consequenties van digitalisering.

4. Meer en andere menskracht Autoriteit Persoonsgegevens
De AP heeft meer en andere menskracht nodig. Vanuit de maatschappij, de rechtspraak en straks ook gesanctioneerd met hulp van de AVG wordt van de AP een strengere rol op het terrein van handhaving verwacht. Op grond van de bevindingen in deze dissertatie betoog ik dat de AP ook data scientists en algoritmisten in dienst zou moeten nemen.
De ACM kan als toezichthouder op het mededingingsrecht aan de AP mogelijk aanvullend – op basis van een effectieve taakverdeling – hulp bieden voor de rechtsbescherming van personen. Illustratief zijn in dit verband de ontwikkelingen in Duitsland. Het mededingingsrecht kan ten dienste staan van informationele zelfbeschikking door samen of afzonderlijk, als dat effectiever is, op te trekken tegen oneigenlijke datamacht.
Wat betreft specifieke wetgeving voorzien van een toezichthoudende rol – dat wil zeggen specifiek in aanvulling op het algemene kader neergelegd in de bestaande AVG en mededingingswetten, valt te denken aan toezicht op de hierna te bespreken wetgeving voor leveranciers van persoonlijke gezondheidsomgevingen.

Tot slot nog twee aanbevelingen voor toekomstige regulering van persoonlijke gezondheidsomgevingen.[696]

5. Patiëntgeheim: aanvullende zwijgplicht en verschoningsrecht
Ik pleit voor een aanvullende wettelijke zwijgplicht voor verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen buiten de behandelrelatie. Een dergelijk patiëntgeheim dient gepaard te gaan met een verschoningsrecht voor leveranciers en gebruikers van persoonlijke gezondheidsomgevingen.

Zoals de Wabvpz te beschouwen is als een aanvulling op de AVG voor elektronische uitwisselingssystemen van zorgaanbieders die binnen de zorg gezondheidsgegevens verwerken, zo kan eveneens aanvullend op de AVG wellicht de zwijgplicht als geheimhoudingsplicht voor verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen geregeld worden. Die wetgeving in aanvulling op de AVG zou tevens personen moeten beschermen tegen derden (gemeenten, UWV, verzekeraars) door welke die personen wel eens onder druk kunnen worden gezet om gebruik te maken van het recht op afschrift van diens medisch dossier om vervolgens die gezondheidsgegevens aan hen te verstrekken.

Om het eerder genoemde 'patiëntgeheim' voor gegevens in gezondheidsomgevingen net zo te regelen als het medisch beroepsgeheim, zal er naast deze geheimhoudingsplicht voor de leverancier een nieuw verschoningsrecht bij de herziening van artikel 218 Sv expliciet meegenomen moeten worden. Daarbij is een omschrijving noodzakelijk die breder is dan stand, ambt en beroep. Ook zal geregeld moeten worden dat het niet alleen natuurlijke personen, maar ook rechtspersonen zijn die zich erop kunnen beroepen.

6. Verbod op het commercieel exploiteren van gezondheidsgegevens
Tot slot het pleidooi om het commercieel exploiteren van gezondheidsgegevens te verbieden. Zoals ook het verhandelen van organen verboden is op grond van de Wet orgaandonatie. Door big-dataprofilering, ondoorzichtige algoritmen en complexe, onzichtbare online datahandel ontstaat een systematische disbalans tussen de machtscapaciteit van bedrijven enerzijds en die van personen anderzijds. Het herstellen van deze disbalans is gewenst. De meerwaarde van een wettelijk verbod op handel in gezondheidsgegevens staat gelet op de datamacht van bedrijven buiten kijf. Hoe dit verbod precies zal moeten worden uitgewerkt, behoeft nader onderzoek. Toestemming op grond van de AVG is een cruciale voorwaarde voor informationele zelfbeschikking, maar biedt onvoldoende garanties.

696. Naast toekomstige regulering van zorggebruikers dient er bij toekomstige regulering in het licht van informationele zelfbeschikking ook rekening te worden gehouden met rechtsbescherming voor zorgaanbieders. Zo is *appen* voor zorgaanbieders een snelle en makkelijke manier om informatie over patiënten te delen. Maar hoe gebeurt zoiets rechtmatig? Dit vraagstuk komt binnen de beperkte omvang van deze dissertatie niet aan de orde en vergt vervolgonderzoek.

Bijlage A *Literatuur*

Aarts, Callen, Coiera & Westbrook 2010
J. Aarts, J. Callen, E. Coiera, and J. Westbrook (2010), *Information technology in health care: socio-technical approaches*,International Journal of Medical Informatics 79 (6): 389-390.

Abel 2003
R.B. Abel (2003), *Geschichte des Datenschutzes*, in: A. Roßnagel (red.), *Handbuch des Datenschutzes*, München: Verlag C.H. Beck, p. 194 e.v.

Actieplan beveiliging patiëntgegevens 2017, Kamerstukken II, 2016/17, 31 765, nr. 259 en 275.

Adams 2006
A. Adams (2006), *Recht en democratie ter discussie. Essays over democratische rechtsvorming*, Leuven: Universitaire Pers, p. 313.

Adams 2010
A. Adams (2010), *De Scheiding der machten tussen feit en fictie. Of: Waarom het soms goed is om in de leugen te leven*, NJB 2010, 227.

Adams & Witteveen 2014
A. Adams en W.J. Witteveen (2014), *Drie dimensies van de rechtsstaat,* NJB 2010, 1017.

Albers 2005
M. Albers (2005), *Informationelle Selbstbestimmung*, Nomos, p. 87 e.v.

Algemene Rekenkamer 2016
Algemene Rekenkamer, Producten op de Europese markt: CE-markering ontrafeld, vastgesteld 21 december 2016 en aangeboden aan de Tweede Kamer 19 januari 2017.

Angrist 2013
M. Angrist (2013), *Genetic privacy needs a More Nuanced Approach*, Nature 494: 7.
Article 29 Working Party. 2004. Working Document on genetic Data. WP91.

Angwin 2014
J. Angwin (2014), *Dragnet Nation. A quest for privacy, security, and freedom ina world of relentless surveillance,* Times Books.

Aubel 1968
C. P. Aubel (1968), *Persoon en pers (diss.),* Deventer: Kluwer.

Bakker 2017
F. Bakker, *Kern van waarheid in rapport HiiL, Mr.* 12 mei 2017.

Balen & Nijveld 2017
C. van Balen en O.S. Nijveld (2017), *De algemene verordening gegevensbescherming: een introductie voor de zorgsector*, TvGR.

Bastiaans 2018
S. Bastiaans (2018), *De inwerkingtreding van de AVG: een dreigend rechtsvacuüm*, NJB 2018, 61.

Barelds e.a 2009
R.J. Barelds e.a. (2009), *Het Persoonlijk Gezondheidsdossier. Een foto van het PGD in Nederland,* TNO-rapport KvL/P&Z 2009.109, in opdracht van Nictiz.

Beauchamp & Childress 2001
T.L. Beauchamp and J.F. Childress (2001), *Principles of Biomedical Ethics,* New York-Oxford: Oxford University Press, p. 58.

Beers 2009
B.C. van Beers (2009), *Persoon en lichaam in het recht, Menselijke waardigheid en zelfbeschikking in het tijdperk van de medische biotechnologie, diss.VU Amsterdam,* Den Haag: Boom Juridische uitgevers, p. 773.

Benda 1984
E. Benda, *Das Recht auf informationelle Selbstbestimmung und die Rechtsprechung des BVerfG zum Datenschutz*, Datenschutz und Datensicherheit, 2: 86-90.

Berkvens & Prins 2007
J.M.A. Berkvens en. J.E.J. Prins, *Privacyregulering in theorie en praktijk,* vierde druk, Deventer: Kluwer.

Berkvens & Jakimowicz 2016
J. Berkvens, C. Jakimowicz (2016), *Tekstuitgave Privacyverordening AVG*, Den Haag: Boom Juridische uitgevers.

Berlin 1958
I. Berlin (1958), *Two concepts of liberty*, in: *Four Essays of Liberty,* Oxford: Oxford University Press.

Beuthien & Schmölz 1999
V. Beuthien & A.S. Schmölz (1999), *Persönlichkeitsschutz durch Persönlichkeitsgüterrechte, Erlösherausgabe statt nur billige Entschädigung in Geld, Information und Recht,* München: Verlag C.H. Beck.

Boyd and Crawford 2012.
D. Boyd & K. Crawford (2012), *Critical questions for Big Data*, Information, Communication and Society, 15 (5): 662-679.

Black 2008
J. Black (2008), *Constructing and contesting legitimacy and accountability in polycentric regulatory regimes*, Regulation & Governance, 2: 137-164.

Blok 2001
P.H. Blok (2001), *De splitsing van privacy. Advies over het grondrecht op privacy in het digitale tijdperk,* AAe, 6 (50): 435-439, m.n. p. 438.

Blok 2002
P.H. Blok (2002), *Het recht op privacy,* Den Haag: Boom Juridische Uitgevers.

Bol 2007
S. Bol (2007), *Mediation en internet: Analyse van juridische* regels *en noodzakelijke waarborgen voor mediation op internet,* Reeks Geschillenbeslechting, Den Haag: Sdu Uitgevers.

Borking 2010
J.J. Borking (2010), *Privacyrecht is code. Over het gebruik van Privacy Enhancing Technologies, diss. Universiteit Leiden,* Deventer: Kluwer.

Borking 2012
J.J. Borking (2012), *Privacy by design,* in: Privacy & Compliance, Tijdschrift voor de praktijk, nr. 03.

Borking 2013
J.J. Borking (2013*), Privacy-by-Design, Haute couture of confectie?*, Computerrecht, nr. 117, p. 186-195.

Brauw de & Van Veen 1965
P.J.W. de Brauw en Th.W. van Veen (1965), *Behoort de wetgever regelen te treffen ter bescherming van de individu tegen het doen, het gebruiken, en het openbaar maken van waarnemingen, diens persoonlijke sfeer betreffende?,* Handelingen der Nederlandse Juristen-Vereniging, Zwolle.

Broeders, Cuijpers & Prins 2011
D. Broeders, M.K.C. Cuijpers en C. Prins (red.) (2011), *De staat van informatie,* Amsterdam: Amsterdam University Press.

Broeders 2005
D. Broeders (2005), *Het geheim in de informatiesamenleving(oratie*), Erasmus Universiteit Rotterdam.

Brownsword 2008
R. Brownsword (2008), *Rights, Regulation, and the Technological Revolution,* Oxford: Oxford University Press.

Brownsword & Yeung 2008,
R. Brownsword and K. Yeung (2008), *Regulating Technologies, Legal futures, regulatory frames and technological fixes,* Oxford and Portland, Oregon: Hart Publishing.

Britz 2008
G. Britz (2008), *Vertraulichkeit und Integrität informationstechnischer Systeme,* DÖV.

Bublitz 2011
J.C. Bublitz (2011), *If a man's true place is in his mind, what is its adequate protection? On a right to mental self-determination and limits of interventions in others minds.* In: *Technologies on the Stand: Legal and ethical questions in neuroscience and robotics, edited by B. van den Berg and L.Klamming*. Nijmegen: Wolf Legal Publishers.

Buitelaar 2012
J.C. Buitelaar (2012), *Back to the Roots*, German Law Journal, 13 (3): 171-202.

Buitelaar 2014
J.C. Buitelaar (2014), *Privacy and Narrativity in the Internet Era*,The Information Society: An International Journal, 30 (4): 266-281.

Butler 2014
D. Butler (2014), *When Google got flu wrong*, Nature 494 (7436): 155-156.

Cameron 2005.
K. Cameron (2005), *The laws of identity*, 2005 https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

Castels 1996
M. Castels (1996), *The Information Age: Economy, Society and Culture. The Rise of the Network Society*. Oxford: Blackwell.

CBP 2012
CBP, 'CBP geeft eerste reactie op nieuwe Europese privacyregelgeving', CBP 25 januari 2012, http://www.cbpweb.nl/Pages/pb_20120125_eerste-reactie-cbp-op-nieuwe-Europese-privacyregelgeving.aspx.

CEG 2014
CEG 2014: 'Leefstijlbeïnvloeding: tussen betuttelen en verwaarlozen', maart 2014.

Cotterrell 1992
R. Cotterrell (1992), *The Sociology of Law. An Introduction,* London, Dublin, Edinburgh: Butterworths.

Cliteur & Van Wissen 2012
P.B. Cliteur en R.G.T. van Wissen (2012), *De menselijke waardigheid als grondslag voor mensenrechten. Een beschouwing over het werk van Kant en Schopenhauer in relatie tot de filosofische reflectie over mensenrechten*, http://www.liberales.be/bestanden/cliteur-waardig.pdf.

Coenraad & Ingelse 2017
L.M. Coenraad en P. Ingelse (2017), *Afscheid van de civiele procedure?,* in: *Afscheid van de klassieke procedure?*, Handelingen NJV 147-II.

Colesky, Hoepman & Hillen 2016
M. Colesky, J. Hoepman en C. Hillen (2016), *A Critical Analysis of Privacy Design Strategies,* IEEE Symposium on Security and Privacy Workshops.

Comijs 2017
D. E. Comijs (2017), *De bescherming van bijzondere persoonsgegevens in de Uitvoeringswet AVG,* NJB 2017, 24.

Comijs 2017b
D.E. Comijs (2017), *Accountability in de AVG: betere processen en een sterkere positie van betrokkenen*, P&I, nr. 253.

Cavoukian 2009
A. Cavoukian (2009), *7 foundational principles Privacy-by-Design*. https://www.ipc.on.ca/wpcontent/uploads/Resources/7foundationalprinciples.pdf.

Condlin 2016
R.J. Condlin (2016), *Online Dispute Resolution: Stinky, Repugnant, or Drab,* University of Maryland Francis King Carey School of Law, Legal Studies Research Paper No. 2016-40.

De Hert 1998
P.J.A. de Hert (1998), *Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak1955-1997,* Antwerpen: Maklu, p. 40-96.

De Hert 2008
P.J.A. de Hert (2008), *A right to identity to face the internet of things?,* Strasbourg: Unesco. http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf.

De Hert, De Vries & Gutwirth 2009
P.J.A. de Hert, K. de Vries en S. Gutwirth (2009), *Duitse rechtspraak over remotesearches, gegevensmining en afluisteren op afstand. Hetarrest Bundesverfassungsgericht 27 februari 2008 (Online Dursuchung) in brederperspectief,* Computerrecht (5): 200-211.

De Hert & Gutwirth 2009
P.J.A. de Hert & S. Gutwirth (2009), *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, in: S. Gutwirth, Y. Poullet, P. de Hert, J.

Nouwt & C. de Terwangne (red.), *Reinventing data protection?,* Dordrecht: Springer Science, p. 3-44.

Delaney 1994
C.F. Delaney (1994), *The liberalism-communitarianism debate: liberty and community values,* Rowman & Littlefield.

DeSimone 2010
C. DeSimone (2010), *Pitting Karlsruhe Against Luxembourg? German Gegevens Protection and the Contested Implementation of the EU Data Retention Directive*, German Law Journal, 11 (3): 291-318.

De Vries 2010
K. de Vries et al (2010), *The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?),* in: S. Gutwirth, *Computer, Privacy and DataProtection: an Element of Choice*.

De Vries, Hooghiemstra, Nouwt en Van Veen 2015
H.H. de Vries, T. Hooghiemstra, J. Nouwt en E.B. van Veen (2015), *Privacydebat ontwikkelingen in de zorg*, P&I, nr. 1, p. 10-13.

Dickie & Yule 2017
N. Dickie en A. Yule (2017), *Privacy by design prevents data headaches later,* Strategic HR Review, 16: 100-101.

Dommering 2010a
E. Dommering, *Recht op persoonsgegevens als zelfbeschikkingsrecht*, in: J.E.J. Prins (red.), *16 miljoen BN'ers? Bescherming van persoonsgegevens in het digitale tijdperk,* Leiden: Stichting NJCM-Boekerij, p. 83-99.

Dommering 2010b
E. Dommering, *Het bestuur van de tovenaarsleerling van ICT*, NJB 2012, 87.

Dommering 2010
E. Dommering (2010), *Recht op persoonsgegevens als zelfbeschikkingsrecht*, in: J.E.J. Prins (red.), *16 miljoen BN'ers? Bescherming van persoonsgegevens in het digitale tijdperk,* Leiden: Stichting NJCM-Boekerij, p. 83-99.
http://www.ivir.nl/publicaties/dommering/NJCM_bundel_2010.pdf.

Dorbeck-Jung en Oude Vrielink-van Heffen 2006
Een nieuwe stijl van reguleren, in: *Op weg naar bruikbare regulering? Themanummer Recht der Werkelijkheid 2006, onder redactie van B. Dorbeck-Jung en M. Oude Vrielink-van Heffen,* Den Haag: Elsevier Juridisch, p. 33-51.

Dorbeck-Jung 2015
B. Dorbeck-Jung (2015), *Bruggen tussen technologieregulering, wetenschap en kunst, (afscheidsrede),* Universiteit Twente.

Durner 2010
W. Durner (2010), *Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet?,* ZUM, p. 833.

Duursma 2017
J. Duursma (2017), *De digitale butler, Kansen en bedreigingen van kunstmatige intelligentie*.

Eberle 1997
E.J. Eberle (1997), *Human Dignity, Privacy and Personality,* Utah L. Rev., p. 963-1056.

Eberle 2001
E.J. Eberle (2001), *The Right to Information Self-Determination,* Utah L. Rev., p. 965.

Eck 2018
B.M.A. van Eck (2018), *Geautomatiseerde ketenbesluiten & rechtsbescherming (proefschrift)*.

Eerste Kamer, 150413EK, Gesprek cliëntenrechten en stand van zaken zorginfrastructuur.

Ehrlich 1975
E. Ehrlich (1975), *Fundamental principles of the sociology of law. Translated by W.L. Moll*. New York: Arno Press.

Engberts 1997
D.P. Engberts (1997), *Morele argumentaties inzake het toestemmingsbeginsel bij de totstandkoming van de Wet Geneeskundige Behandelings-Overeenkomst (diss. Universiteit Leiden),* Deventer: Kluwer.

ENISA 2012 Study on monetizing privacy. An economic model for pricing personal information.

European Commission 2012, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 2012/0011.

European Network of Councils for the Judiciary (ENJC), *Accountability and Quality of the Judiciary Performance Indicators 2017*, ENJC report 2016-2017, June 2017.

COM(2015) 192, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe (*Digital Single Market*).

Eifert 2008
M. Eifert (2008), *Informationelle Selbstbestimmung im Internet. Das BVerfG und die Online-Durchsuchungen,* NVwZ, p. 521.

Elwyn 2012
G. Elwyn, D.L. Frosch en S. Kobrin (2012), *Implementing shared decision-making: consider all the consequences*, IS 2015, 11: 114.

Elwyn 2014
G. Elwyn, A. Lloyd, C. May, T. van der Weijden, A. Stiggelbout, A. Edwards, et al. (2014), *Collaborative deliberation: A model for patient care,*Patient Education and Counseling, 97: 158-64.

Elwyn 2015
G. Elwyn, D.L. Frosch, S. Kobrin (2015), *Implementing shared decision-making: consider all the consequences*, IS 2015 11: 114.

ENISA, Privacy by Design in big data – an overview of privacy enhancing technologies in the era of big data analytics, December 2015.

Ermert 2008
M. Ermert (2008), *Datenschutz trotz 25 Jahren informationeller Selbstbestimmung noch unzureichend,* Heise Online. 15 december 2008. http://www.bfdi.bund.de/cae/servlet/contentblob/561720/publicationFile/31309/Dokumentation25JahreVolkszaehlungsurteil.pdf.

Expertgroep Big data en privacy voor minister van Economische Zaken, Licht op de digitale schaduw, verantwoord innoveren met big data, augustus 2016.

Fisahn & Kutscha 2011
A. Fisahn & M. Kutscha (2011), *Verfassungsrecht konkret: Die Grundrechte*, BWV, p. 6.

Franken, Kaspersen en de Wild 2004
H. Franken, H.W.K. Kaspersen en A.H. de Wild (2004), *Recht en Computer*, Deventer: Kluwer.

French 2014
M. French (2014), *Gaps in the gaze: information practice and the work of public health surveillance*, Surveillance & Society, 12 (2): 226-243.

Friedman 1975
L.M. Friedman (1975), *The Legal System; A Social Science Perspective,* New York: Russell Sage Foundation.

Friedman 1990
L.M. Friedman (1990), *The Republic of Choice. Law, Authority and Choice,* Cambridge (Mass.): Harvard U.P., p. 184.

Fuller 1969
L. Fuller (1969), *The Morality of law, revisited edition*. New Haven en London: Yale University Press.

Gallwas 1992
H. Gallwas (1992), *Der allgemeine Konflikt zwischen dem Recht auf informationelle Selbstbestimmung und der Informationsfreiheit*, NJW, p. 2785-2848.

Garton-Ash 2013
T. Garton-Ash (2013), *If Big Brother came back, he'd be a public private partnership,* The Guardian, 27 June, 2013, Opinion page.

Gellman
R. Gellman, *Personal Health Records: Why Many PHRs Threaten Privacy,* Prepared for the World Privacy.

Gezondheidsraad 2004
Gezondheidsraad, Advies Bewaartermijnen Patiëntengegevens, 1 april 2004.

GfK: Willingness to share personal data in exchange for benefits or rewards, Global GfK survey, January 2017.

Gold 2012
M.K. Gold e.a. (2012), *Debates in the Digital Humanities,* Minneapolis: University of Minnesota Press.

Gola & Schomerus 2012
P. Gola en R. Schomerus (2012), *BDSG Bundesdatenschutzgesetz,* §1 Zweck und Anwendungsbereich, nr. 9-13.

Goodman 2015
M. Goodman (2015), *Future Crimes, A Journey to the Dark Side of Technology – And How to Survive it*.

Green 2001
I. Green (2001), *Communication, technology and Society*. London: Sage publications.

Griffiths 1996
J. Griffiths (1996), *De sociale werking van recht*, in: J. Griffiths & H. Weyers (red), *De sociale werking van recht. Een kennismaking met de rechtssociologie en rechtsantropologie,* Nijmegen: Ars Aequi libri, p. 469-514.

Guthwirth e.a. 2011
Gutwirth, S., R. Gellert, R. Bellanova, M. Friedewald, P. Schutz, D. Wright, E. Mordini en S. Venier (2011), *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies* in: *PRESCIENT project (D2),* Karlsruhe: Frainhofer ISI.

Götting 2008
H. Götting, in: H. Götting, C. Schertz & W. Seitz (2008), *Handbuch des Persönlichkeitsrechts,* §3, Rdnr. 4, 6.

Hallinan 2014
D. Hallinan, P. Schutz, M. Friedewald en P. de Hert (2014), *Neurodata en Neuroprivacy. Data ProtectionOutdated?*, Surveillance & Society, 1291: 55-72.

Harari 2017
Y.N. Harari (2017), *Homo Deus, een kleine geschiedenis van de toekomst,* Thomas Rap.

Havinga, Klaassen en Neelis 2012
T. Havinga, C. Klaassen en N. Neelis (2012), *Specialisatie gewenst?De behoefte aan gespecialiseerde rechtspraak binnen het Nederlandse bedrijfsleven,* Raad voor de Rechtspraak.

HEC 2010
R.A.E. Gerads, T.F.M. Hooghiemstra, A.G. Arnold, A.D. van der Heide (2010), *De informatiepositie van de patiënt*, HEC, Den Haag: Sdu Uitgevers.

Heckmann 2006
D. Heckmann (2006), *Präventive polizeiliche Rasterfahndung*, JurisPR-ITR (6).

Heijna 2017
R.C. Heijna (2017), *Verslag VPR-debat Uitvoeringswet AVG d.d. 10 januari 2017,* P&I 5 (1).

Hendriks 2006
A. Hendriks (2006), *In beginsel, de gezondheidsrechtelijke beginselen uitgediept,* Leiden: Stichting NJCM-Boekerij, p. 5.

Hendriks 2008
A.C. Hendriks, B.J.M. Verkerk, M.A. (2008), *Het recht op autonomie in samenhang metgoede zorg bezien*, TvGR, nr. 32, p. 2-18.

Hendriks 2010
A.C. Hendriks (2010), *boekbespreking dissertatie B.C. van Beers,* TvCR, p. 353-357.

Hendriks (red.) 2013
A.C. Hendriks, R.D. Friele, J. Legemaate, G.A.M. Widdershoven (2013), *Thematische wetsevaluatie zelfbeschikking in de zorg*. 8.4.1. Informationele zelfbeschikking, p. 204-2012.

Hertogh & Weyers 2011
M. Hertogh & H. Weyers (2011), *Recht van onderop, antwoorden uit de rechtssociologie,* Nijmegen: Ars Aequi Libri.

Herveg 2009
J. Herveg (2009), *Chronicle of Case-Law: The European Court of Human Rights and the Protection of Patiënt'sData (1st January 2000 – 24 June 2009)*.
http://works.bepress.com/cgi/viewcontent.cgi?article=1010&context=jean_herveg.

Hes & Borking 2010
R. Hes & J. Borking (2010), *Privacy-enhancing-technologies, The path to anonymity, Revised Edition,* Registratiekamer 2010.

HiiL, Barendrecht, Van Beek & Muller, 2017
M. Barendrecht, K. van Beek en S. Muller (2017), *Menselijk en rechtvaardig. Is de rechtsstaatervoorde burger?,* HiiL.

Hijmans 2016
H. Hijmans, *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU (diss.),* University of Amsterdam.

Hijmans 2018
H. Hijmans (2018), *De AVG en de UAVG*, NJB 2018, 356.

Hildebrandt & Van Dijk 2010
M. Hildebrandt & N. van Dijk (2010), *Klantenprofielen: de onzichtbare hand van internet*, in: G. Munnichs, M. Schuiff en M. Besters (red), *Databases. Over ICT-beloftes, informatiehongeren digitale autonomie,* Den Haag: Rathenau Instituut.

Hildebrandt 2011
M. Hildebrandt (2011), *De rechtsstaat in cyberspace?,* Deventer: Kluwer.

Hildebrandt, Leenes en Lokin 2012
M. Hildebrandt, R.E. Leenes en M.H.A.F. Lokin (2012), *Technologie en wetgeving in cyberspace: verstandshuwelijk of innige relatie?,* Den Haag: Boom Juridische uitgevers, RegelMaat 2012/2, p. 61-75.

Hirsch Ballin 1993
E.M.H. Hirsch Ballin (1993), *De staat van Nederland,* Tilburg: Tilburg University Press.

Hirsch Ballin 2016
E.M.H. Hirsch Ballin (2016), *Big Data in een vrije en veilige samenleving,* TMC, nr. 4, p. 101.

Hobbes 1651
T. Hobbes (1652), *Leviathan, or The Matter, Form & Power of a Common-Wealth Ecclesiastical and Civil.*

Hoepman 2012
J.H. Hoepman (2012), *Privacy design strategies*.
http://arxiv.org/pdf/1210.6621.pdf.

Hoepman & Hooghiemstra 2012
J.H. Hoepman en T.F.M. Hooghiemstra (2012), *Goede code, De Digitale samenleving in balans,* Regelmaat 27 (2), p. 76-87.

Hoepman 2014
J.H. Hoepman, *Privacy Design Strategies,* in: *IFIP TC11 29th Int. Conf. on Information Security,* IFIP SEC,, p. 446-459.

Hoffmann-Riem 1998
W. Hoffmann-Riem (1998), *Informationelle Selbstbestimmung in der Informationsgesellschaft*, 123 AöR1998.

Hoffmann-Riem 2008
W. Hoffmann-Riem (2008), *Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme,* 21 JZ2008, p. 1009-1060.

Holvast, 2016
J. Holvast (2016), *Algemene verordening gegevensbescherming: veel gespin en weinig wol*, P&I 103 (3).

Hooghiemstra 1998
T.F.M Hooghiemstra (1998), *Privacy & Managed Care,* Den Haag: Registratiekamer.

Hooghiemstra 1999
T.F.M. Hooghiemstra (1999), *De Wet bescherming persoonsgegevens en de gezondheidszorg,* TvGR, p. 17-27.

Hooghiemstra 2007
T.F.M. Hooghiemstra (2007), *Zelfbeschikking bij ICT en het medisch dossier*, P&I, p. 254.

Hooghiemstra & Gerards 2010
T.F.M. Hooghiemstra en R. Gerards (2010), *De informatiepositie van de patiënt*, P&I, p. 51.

Hooghiemstra 2011
T.F.M. Hooghiemstra en J. Nouwt (2011), *eHealth en recht. Inleiding op het thema,* Computerrecht, nr. 6, p. 289.

Hooghiemstra & Ippel 2011
T.F.M. Hooghiemstra en P. Ippel (2011), *Zeggenschap over het EPD, ethisch en juridisch perspectief,* Centrum voor ethiek en gezondheid (CEG).

Hooghiemstra & Nouwt 2014
T. Hooghiemstra en S. Nouwt (2014), *Een juridische blik op trends in e-health*, Nederlands tijdschrift voor Geneeskunde.

Hooghiemstra & Nouwt 2017
T.F.M. Hooghiemstra en S. Nouwt (2017), *Commentaar Wet bescherming persoonsgegevens,* Den Haag: Sdu Uitgevers.

Hooghiemstra & Nouwt 2018a
T.F.M. Hooghiemstra en S. Nouwt (2018), *Annotatie bij HR 1 december 2017, ECLI:NL:HR:2017:3053 (LSP)*, JBP 2018/4, Sdu Jurisprudentie Bescherming Persoonsgegevens, afl. 1, 2018.

Hooghiemstra & Nouwt 2018b
T.F.M. Hooghiemstra en S. Nouwt (2018), *Commentaar AVG,* Den Haag: Sdu Uitgevers.

Hornung en Schnabel 2009
G. Hornung and C. Schnabel (2009), *Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,* Computer Law & Security Review 25 (2), 115-122.

Hornung 2007
G. Hornung (2007), *Ermächtigungsgrundlage für die 'Online-Durchsuchung*?, Datenschutz und Datensicherheit, p. 575 e.v.

Hornung 2008
G. Hornung (2008), *Ein neues Grundrecht*, Computer und Recht, p. 299 e.v.

Hornung & Schnabel 2009a
G. Hornung en C. Schnabel (2009), *Data protection in Germany I: The population census decision and the right to informational self-determination*, 25 Computer Law & Security Review, p. 84-88.

Hornung & Schnabel 2009b
G. Hornung en C. Schnabel (2009), *Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,* 25 Computer Law & Security Review, p. 115.

Hornung, Bendrath & Pfitzmann 2010
G. Hornung, R. Bendrath en A. Pfitzmann (2010), *Surveillance in Germany: Strategies and Counterstrategies*, in: S. Gutwirth, Y. Poullet & P. de Hert (eds.),*Data Protection in a Profiled World,* Dordrecht: Springer, p. 139-156.

Huber 2011
M. Huber (2011), *How shall we define health?*, British Medical Journal, 343:d4163.

Hulst & Van den Bos 2017
L. Hulst & K. van den Bos (2017), *Is de Nederlandse rechtsstaat echt doof, blind, vastgeroest, onmenselijk en onrechtvaardig?: Weloverwogen, en niet overhaast, op weg naar responsievere rechtspleging*, NJB 2017, 1457.

Hustinx 1973
P.J. Hustinx (1973), *De bescherming van de persoonlijke levenssfeer bij de toepassing van de computer, Preadvies Vereniging voor de Vergelijkende Studie van het Recht van Nederland en België,* Zwolle, p. 11.

Hustinx 1999
P.J. Hustinx (1999), *Informatietechnologie in de gezondheidszorg. Preadvies voor de vergadering van de Vereniging voor Gezondheidsrecht.*

Hustinx 2002
P.J. Hustinx (2002), *Privacy, Data Protection and Informational Selfdetermination,* Conference of Dataprotection Authorities, Athene.

Hustinx 2005
P.J. Hustinx (2005), *Data protection in the European Union,* P&I, nr. 2, p. 62-65.

Hustinx 2010
P. Hustinx (2010), *Privacy by design: delivering the promises,* Identity in the Information Society, 3 (2): 253–255.

Hustinx 2017
P. Hustinx (2017), *EU Data Protection Law*, in: L. Azoulai, N. Bhuta, M. Cremona, *The Collected Courses of the Academy of European Law*, New Technologies and EU Law, Volume XXIV/2, p. 123-174.

Ihde 1990
D. Ihde (1990), *Technology and the Lifeworld; From garden to earth,* Bloomington: Indiana University Press.

Ioannidis
J.P.A. Ioannidis, *Why Most Published Research Findings Are False,* plos Med 2 (8):e124.

Ippel 1987
P.C. Ippel (1987), *klachtbehandeling en klachtprocedures*, Zwolle: W.E.J. Tjeenk Willink.

Ippel 2002
P.C. Ippel (2002), *Modern recht en het goede leven, over gezondheid, milieu en privacy,* Den Haag: Boom Juridische Uitgevers.

Jacobs 2015
B. Jacobs (2015), *Voorwoord in:* Marcel Becker, *Ethiek van de digitale media*, Den Haag: Boom Juridische uitgevers.
http://pilab.nl/about%20pi%20lab/blog/preface%20from%20marcel%20becker.html.

Jacobs 2017
B. Jacobs (2017), *Zonder privacy is er geen er geen vrijheid,* Trouw, 23 april 2017.

Jansen & Wolters 2017
C.J.H. Jansen en P.T.J. Wolters (2017), *Ieder bedrijf heeft digitale zorgplichten: Een handreiking voor bedrijven op het gebied van cybersecurity),* Cyber Security Raad.

Kannekens & Van Eijk 2016
E. Kannekens en N. van Eijk (2016), *Oneerlijke handelspraktijken: alternatief voor privacyhandhaving,* TMC, nr. 4, p. 102.

Kant 1781
I. Kant (1781), *Kritiek van de zuivere rede*.

Kant 1785
I. Kant (1785), *Grundlegung zur Metaphysik der Sitten,* Werkausgabe, Band VII, Hrsg.W.

Katsh & Rifkin 2001
E. Katch en J. Rifkin (2001), *Digital Justice: Technology and the Internet of Disputes*.

Katch & Rifkin 2001
E. Katsh en J. Rifkin (2001), *Online Dispute Resolution: Resolving Conflicts in Cyberspace,* San Francisco: Jossey-Bass.

Katch & Rabinovich-Einy 2017
E. Katsch en O. Rabinovich-Einy (2017), *Digital Justice: Technology and the Internet of Disputes*.

Kayyali, Knott & van Kuiken 2013.
B. Kayyali, D. Knott en S. van Kuiken (2013), *The big-data revolution in US health care: Accelerating value and innovation,* New York: McKinsey & Company.

Kipker & Schaar 2017
D.K. Kipker en P. Schaar (2017), *Vernetzte medizinische Forschung und Datenschutz,* ZD-Aktuell 2017, 04263.

Kits 2017
P.M. Kits (2017), *Big data en privacy. Luctor et emergo? In Deel 1 Gegevenszee en het privacybegrip, preadvies Big data in de zorg,* Vereniging voor Gezondheidsrecht, p. 56-57.

Klous & N. Wielaart 2014
S. Klous & N. Wielaart (2014), *Wij zijn Big Data: de toekomst van Big Data,* Business Contact.

Klauser & Albrechtslund 2014
F.R. Klauser & A. Albrechtslund (2014), *From self-tracking to smart urban infrastructures: towards an interdisciplinary research agenda on Big Data*, Surveillance & Society, 12 (2): 273-286.

Kranenborg & Verhey 2011
H.R. Kranenborg en L.F.M. Verhey (2011), *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer.

KNMG Handreiking 'Beroepsgeheim en politie/justitie', 2012.

KNMG Richtlijn 'omgaan met medische gegevens', 2010.

KNMG Richtlijn 'omgaan met medische gegevens', 2016.

Koekkoek 2000
A.K. Koekkoek e.a. (2000), *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport,* Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Justitie ten behoeve van de Commissie Grondrechten in het digitale tijdperk.

Kool & Van Est 2014
L. Kool en Q.C. van Est (2014), *Intieme technologie : grip gewenst op het web rondom onze biologische data*, Liberaal Reveil, 55 (4): 173-179.

Kool, Timmer, Royakkers, Van Est 2017
L. Kool, J. Timmer, L. Royakkers en R. van Est (2017), *Opwaarderen - Borgen van publieke waarden in de digitale samenleving,* Den Haag: Rathenau Instituut.

Koops 2010
B.J. Koops (2010), *Het failliet van het grondrecht op gegevensprotectie*, in: J.E.J. Prins (red.), *16 miljoen BN'ers? Bescherming van persoonsgegevens in het digitale tijdperk,* Leiden: Stichting NJCM-Boekerij, p. 99 e.v.

Koops 2011
E.J. Koops (2011), *Digitale grondrechten en de Staatscommissie: Op zoek naar de kern,* Tijdschrift voor constitutioneel recht, 2 (2): 168-185.

Koops 2014
B.J. Koops (2014), *The trouble with European Data Protection Law,* International Data Privacy Law. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692.

Koops & Leenes, 2014
B.J. Koops en R.E. Leenes (2014), *Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law,* International Review of Law, Computers & Technology, nr. 2.

Kors 1981
A. Kors (1981), *Recht op onaantastbaarheid van het menselijk lichaam*, NCJM-bull, p. 106-115.

Kosta & Stuurman 2015
E. Kosta en C. Stuurman (2015), *Technical standards and the draft general data protection regulation*, in: *The Law, Economics and Politics of International Standardization. Panagiotis, D. (ed.),* Cambridge University Press, p. 434-459.

Kurzweil 2006
R. Kurzweil (2006), *The Singularity is Near, When Humans Transcent Biology*.

Kutscha 2012
M. Kutscha (2012), *Das "Computer-Grundrecht" – eine Erfolgsgeschichte?,* Datenschutz und Datensicherheit, nr. 6, p. 391-394.

Latour 2005
B. Latour (2005), *Reassembling the Social. An introduction to Actor-Network-Theory,* Oxford: Oxford University Press, (Weischedel, Suhrkamp, Frankfurt am Main, 1981), p. 68.

Leenen & Gevers 2000
H.J.J. Leenen en J.K.M Gevers (2000), *Handboek Gezondheidsrecht, Deel I, Rechten van mensen in de gezondheidszorg, vierde druk*, Houten/Diegem: Bohn Stafleu Van Loghum, p. 11.

Leenen, Dute, Gevers, Legemaate, Groot, Gelpke & de Jong 2017
H.J.J. Leenen, J.C.J Dute, J.K.M. Gevers, J. Legemaate, G.R.J. Groot, M.E. Gelpke, E.J.C. de Jong (2017), *Handboek gezondheidsrecht,* zevende druk, Boom Juridische uitgevers.

Leenes 2010
R. Leenes (2010), *Harde lessen. Apologie voor technologie als reguleringsinstrument*.

Leenes 2014
R. Leenes (2014), *Actieplan Privacy 2014*.

Legg 2016
M. Legg (2016), *The Future of Dispute Resolution: Online ADR and Online Courts, Forthcoming Australasian Dispute Resolution Journal*.

Lepsius 2008
O. Lepsius (2008), *Das Computer-Grundrecht*, in: F. Roggan (Hrsg.), *Online-Durchsuchungen*.

Lessig 2006
L. Lessig (2006), *Code and Other Laws of Cyberspace*. New York: Basic Books 1999 en recenter: L. Lessig, *Code version 2.0,* New York: Basic Books.

Lokin & Zandbergen 2017
M.H.A.F Lokin en T. Zandbergen (2017), *Digitaal 2017: ontwikkelingen in elektronische communicatie met de overheid, in het bijzonder de Belastingdienst*, MBB, nr. 7-8.

Looney, Kidmose, Park, Ungstrup, Rank, Rosenkranz & Mandic 2012
D. Looney, P. Kidmose, C. Park, M. Ungstrup, M.L. Rank, K. Rosenkranz and D.P. Mandic (2012), *The In-the-Ear Recording Concept: User-centered and Wearable Brain Monitoring,* IEEE Pulse 3 (6): 32-42.

Lousberg & Cuijpers 2017
Mr. J. Lousberg, dr. C. Cuijpers (2017), *Het recht op vergeten en Google,* P&I, *nr.* 209.

Ludz 1976
P. Ludz (1976), *Alienation as a concept in the social sciences*, in: R. Greyer & D. Schweizer (eds), *Theories of alienation: critical perspectives in philosophy and the social sciences,* Leiden: Martinus Nijhoff, p. 3-37.

Luhmann 1965
N. Luhmann (1965), *Grundrechte als Institution: Ein Beitrag zur politischen Soziologie,* Berlin: Duncker & Humblot.

Luijtgaarden 2017
E. van de Luijtgaarden (2017), *Preventive Law, Aanzet tot normatieve professionalisering in de opleiding van juristen*,Aspekt, 2017.

Makoul 2006
G. Makoul & M.L. Clayman (2006), *An integrative model of shared decision making in medical encounters*,*Patient Education and Counseling*, 60: 301-312.

Markenstein 2005
L.F. Markenstein (2005), *Tekst en toelichting WGBO. Editie 2006,* Den Haag: Sdu Uitgevers, p. 36.

Martijn en Tokmetzis 2016
M. Martijn en D. Tokmetzis (2016), *Je hebt wel iets te verbergen, over het levensbelang van privacy,* De Correspondent.

Marx 1884
K. Marx (1884), *Early Writings (Translated and edited by T.B. Bottomore),* New York: McGraw-Hill Book Company 1964 (Economic and Philosophical Manuscripts (1884), First Manuscript, XXII. 'Alienated Labour').

Mayer-Schoenberger and Cukier 2013
V. Mayer-Schoenberger and K. Cukier (2013), *Big Data. A Revolution that will transform how we live, work and think,* London: John Murray Publishers.

Mascini & Van Erp 2011
P. Mascini & J. van Erp (2011), *Waarom zijn sommige vormen van rechtshandhaving effectiever dan andere?,* in: M. Hertogh en H. Weyers, *Recht van onderop, Antwoorden uit de rechtssociologie*, Nijmegen: Ars Aequi Libri.

Meijenfeldt 2017
L.H. von Meijenfeldt (2017), *De AVG en Awb: vragen om Babylonische spraakverwarring,* P&I, 107, nr. 3.

Meissner 2017
S. Meissner (2017), *The Merits of data protection certification under GDPR,* Tribune Libre, nr. 19.

Mersch 2018
M.F. van der Mersch (2018), *Nieuwe E-health toepassingen, zijn de patiëntenrechten aan innovatie toe?*, in: *Nieuwe techniek, nieuwe zorg, preadvies,* Vereniging voor Gezondheidsrecht.

Michael & Michael 2009
K. Michael en M.G. Michael (2009), *Innovative automatic identification and location-based services: from bar codes to chip implants,* IGI Global.

Mill 1859
J.S. Mill (1859), *On Liberty,* Harmondsworth: Penguin Books 1859 (1979), p. 68-69.

Milne & Culnan 2004
G. Milne M. Culnan (2004), *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices,* 18 Journal of Interactive Marketing, 15.

Moerel 2010
L. Moerel (2010), *The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?,* International Data Privacy Law, p. 1-19.

Moerel 2014
L. Moerel (2014), *Big Data Protection, How to Make the Draft EU Regulation on Data Protection Future Proof(Oratie),* Universiteit Tilburg.
http://www.mondaq.com/x/298416/data+protection/Big+Data+Protection+How+To+Make+The+Draft+EU+Regulation+On+Data+Protection+Future+Proof al Lecture.

Moerel & Prins 2016
E.M.L. Moerel en J.E.J. Prins (2016), *Privacy voor de homo digitalis*, in: *Homo Digitalis. Preadviezen(Handelingen Nederlandse Juristenvereniging, deel 2016 I)*, Deventer: Wolters Kluwer.

Moore 2014
S. Moore (2014), *Recht en maatschappelijke verandering*, in: J. Griffiths & H. Oostveen, A., A. Vasalou, P. van den Besselaar en I. Brown.*Child Location Tracking in the US and the UK: Same Technology, Different Social Implications,* Surveillance & Society, 12 (4): 581-593.

De Mul, 2016
J. de Mul (2016), *Kunstmatig van nature, onderweg naar Homo sapiens 3.0,* Rotterdam: Lemniscaat.

Mulder & Borking, 2006
J.B.F. Mulder en J.J. Borking (2006), *De eerste praktische ervaringen met elektronische geschillenoplossing in Nederland,* Computerrecht, nr. 5, p. 255-259.

Mulley 2012
A.G. Mulley, C. Trimble, G. Elwyn (2012), *Stop the silent misdiagnosis: patients' preferences matter,* British Medical Journal, 345: e6572-5.

Nature: Editorial 2013. *Genetic privacy*. Nature 493: 451.

Nehmelmann 2002
R. Nehmelmann (2002), *Het algemeen persoonlijkheidsrecht. Een rechtsvergelijkende studie naar het algemeen persoonlijkheidsrecht in Duitsland en Nederland*.

Nissenbaum 2004
H. Nissenbaum (2004), *Privacy as contextual integrity*, 19 Washington Law Review 119.

Nissenbaum 2010
H. Nissenbaum (2010), *Privacy in Context: technology, policy and the integrity of social life,* Stanford: Stanford University Press.

Nissenbaum 2011
H. Nissenbaum (2011), *A Contextual Approach to Privacy Online,* Daedalus, 140 (4): 32-48.

Noordegraaf 2008
M. Noordegraaf (2008), *Management in het publieke domein, Issues, instituties en instrumenten,* Countinho.

NHG 2016
NHG, Richtlijn gegevensuitwisseling huisarts-centrale huisartsenpost, versie 5, 2016.

Nieuwenhuis 2001
A.J. Nieuwenhuis (2001), *Tussen privacy en persoonlijkheidsrecht. Een grondrechtelijk en rechtsvergelijkend onderzoek,* Nijmegen: Ars Aequi Libri.

Nieuwenhuis, Den Heijer & Hins 2014
A.J. Nieuwenhuis, M. den Heijer en A.W. Hins (2014), *Hoofdstukken grondrechten,* Nijmegen: Ars Aequi Libri.

Nissenbaum 2010
H. Nissenbaum (2010), *Privacy in context: technology, policy, and the integrity of social life, Standford:* Stanford University Press.

NIVEL 2011
A.E.M. Brabers, M. Reitsma-van Rooijen, J.D. de Jong (2011), *Consumentenpanel Gezondheidszorg,* Utrecht: NIVEL.

Nonet &Selznick 2001
P. Nonet and P. Selznick (2001), *Law and society in transition: toward responsive law*.

Nouwt 1997
S. Nouwt (1997), *Zorg voor privacy(dissertatie),* Tilburg.

Nouwt 2016a
S. Nouwt (2016), *WhatsApp in de zorg, veilig of niet?,* Tijdschrift Zorg & recht in de praktijk, nr. 6, p. 20-23.

Nouwt 2016b
J. Nouwt (2016), *Naar een recht op elektronische inzage in het medisch dossier*, P&I 252, nr. 6.

Nouwt 2018
J. Nouwt (2018), *Berichten uit Brussel, Richtlijnen over de AVG,* P&I, nr. 1, p. 5-11.

Oosterlaken & Van den Hoven 2012
I. Oosterlaken en J. van den Hoven (2012), *The CapabilityApproach, Technology and Design,* Springer.

Ottes 2017
L. Ottes e.a., *Big Data in de zorg, Preadvies,* Vereniging voor Gezondheidsrecht.

Overkleeft-Verburg 2000
G. Overkleeft-Verburg (2000), *Het grondrecht op eerbiediging van de persoonlijke levenssfeer*', in: A.K. Koekoek (red.), *De Grondwet. Een systematisch en artikelsgewijs commentaar,* Deventer: Kluwer, p. 155-178.

PBLQ 2016
Onderzoek van PBLQ in opdracht van de minister van VWS naar de beveiliging van patiëntgegevens bij zorginstellingen, inclusief reactie van minister aan parlement, december 2016, Kamerstukken II, 2016-2017, 31 765, nr. 259. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z24031&did=2016D49230.

Pieroth & Schlink 1996
B. Pieroth en B. Schlink (1996), *Grundrechte Staatsrecht II,* Rdnr. 414.

Pieroth & Schlink 2006
B. Pieroth en B. Schlink (2006), *Grundrechte Staatsrecht II,* Rdnr. 373 e.v.

Pieroth & Schlink 2008
B. Pieroth en B. Schlink (2008), *Grundrechte Staatsrecht II,* § 4, Rdnr. 79 e.v.

Ploem & Dute 2014
M.C. Ploem en J.C.J. Dute (2014), *Hetjuridischkadervoor 'healthchecks*': balanceren tussen vrijheid en bescherming', TvGR, nr. 8, p. 2-14.

Ploem 1999
M.C. Ploem (1999), *Weergave van de discussie naar aanleiding van het preadvies van P.J. Hustinx,* TvGR, p. 301-305.

Pluut 2017
B. Pluut (2017), *The unfolding of discursive struggles in the context of Health Information Exchange (doctoral thesis),* Universiteit Utrecht.

Ploem, Dute 2014
M.C. Ploem en J.C.J. Dute (2014), *Het juridisch kader voor 'healthchecks': balanceren tussen vrijheid en bescherming*, TvGR, nr. 8.

Posner 1981
R.A. Posner (1981), *The Economics of privacy*, 71 The American Economic Review, p. 405 e.v.

Posner 1983
R.A. Posner (1983), *Privacy as secrecy*, in: R.A. Posner, *The Economics of justice,* Massachusetts/London: Harvard University Press, p. 231 e.v.

Prins 2006
J.E.J. Prins (2006), *Property and Privacy; European Perspectives and the Commodification of Our Identity,* in: *The Future of the Public Domain, Identifying the Commons in Information Law*, Deventer: Kluwer Law International, p. 223-57.

Prins 2010
J.E.J. Prins (2010), *Burgers en Hun Privacy: Over Verhouding en Houding Tot een Ongemakkelijk Bezit,* in: *Bescherming van persoonsgegevens in het digitale tijdperk,* Leiden: Stichting NJCM.

Prins 2016
J.E.J. Prins (2016), *Inleiding pre-adviseurs*, in: *Homo Digitalis. Verslag van de op 10 juni 2016 te Haarlem gehouden algemene vergadering (Handelingen Nederlandse Juristenvereniging, deel 2016 II),* Deventer: Wolters Kluwer.

Prins 2017
J.E.J. Prins (2017), *Cybersecurity en zorgplichten*, NJB 2017, 841.

PrivacyCare & PBLQ 2016
J. Krabben en T.F.M. Hooghiemstra (2016), *Betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de Zorg in opdracht van de minister van VWS*.

Raab & Szekely, 2017
C. Raab en I. Szekely (2017), *Data protection authorities and informationTechnology,* Computer Law & Security Review, nr. 33, p. 421-433.

Radbruch 1945
G. Radbruch (1945), *Fünf Minuten Rechtsphilosophie*, in*: Rhein_Neckar-Zeitung vom 12.9.1945, zittiert nach dem Neuabdruck in: ders., rechtsphilosophie, *Aufl, hrsgg, von Erik Wolf und Hans-peter Schneider,* Stuttgart, S.327 ff.

Rifkin 2001
J. Rifkin (2001), *Online Dispute Resolution: Theory and Practice of the Fourth Party*, 19(1) Conflict Resolution, Quarterly 117 at 119.

Rigaux 1990
F. Rigaux (1990), *La protection de la vie privée et des autres biens de la personnalité,* Bruxelles-Paris: Bruylant 1990, p. 167.

RLI: Doen en laten, effectiever milieubeleid door mensenkennis, maart 2014.

RMO, De verleiding weerstaan, Grenzen aan beïnvloeding van gedrag door de overheid, maart 2014.

Rogers 2003
E.M. Rogers (2003), *Diffusion of Innovations, 5th edition,* New York.

Rodota 1995
S. Rodotà (1995), *Technologie e diritti, Il Mulino,* Bologna, p. 122.

Rodota 2009
S. Rodotà (2009), *Databescherming als Fundamenteel Recht*, in: S. Gutwirth e.a.,*Reinventing Data Protection*, p. 79-80.

Ronnellenfitsch 2009
M. Ronnellenfitsch (2009), *Der Vorrang des Grundrechts auf informationelle Selbstbestimmung vor dem AEUV*, Datenschutz und Datensicherheit, nr. 8, p. 451-461.

Rooy & Bus 2009
D. van Rooy en J. Bus (2009), *Informal note on privacy & identity in the digital society & economy in response to the guiding questions of the draft agenda,* Oxford.

Rosen 2000
J. Rosen, The Unwanted Gaze (2000), *The Destruction of Privacy in America,* New York: Random House, p. 20.

Roßnagel & Schnabel 2008
A. Roßnagel en C. Schnabel (2008), *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht,* NJW, p. 3534-3538.

Rouvroy & Poullet 2009
A. Rouvory en Y. Poullet (2009), *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, in: S. Gutwirth e.a., *Reinventing Data Protection*.

RVZ 2013
De participerende patiënt, Den Haag 2013.

RVZ 2014
Patiënteninformatie, Informatievoorziening rondom de patiënt, Den Haag, juli 2014.

RVZ 2015
Consumenten eHealth, Den Haag 2015.

Salter 2017
S. Salter (2017), *ODR and Justice System Integration: B.C.'s Civil Resolution Tribunal*, Windsor Yearbook of Access to Justice, 34 (1).

Scheltema, 2015 a
M. Scheltema (2015), *Bureaucratische rechtsstaat of responsieve rechtsstaat?,* NTB, nr. 9, p. 287-289.

Scheltema 2015b
M. Scheltema (2015), *Rechtseenheid of rechtsstaat als doelstelling van de Awb?*, NJB 2015, 814.

Schermer, Hagenauw & Falot 2018
B.W. Schermer, D. Hagenauw, N. Falot (2018), *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming,* Den Haag: Ministerie van Justitie en Veiligheid.

Schmidt & Cohen 2013
Schmidt, E. and J. Cohen (2013), *The New Digital Age. Reshaping the Future of People,* Nations and Business, New York: Knopf.

Schnitzler 2015
H. Schnitzler (2015), *Het digitale proletariaat,* De bezige bij.

Schuyt 1983
K. Schuyt (1983), *Recht en Samenleving*.

Schwartz 1989
P. Schwartz (1989), *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination,* 37 The American Journal of Comparative Law (4), p. 675-701.

Schwartz 2011
P. Schwartz (2011), *Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, The State, and New Technology,* 53 William and Mary Law Review, p. 351-387.

Schulz 2012
G. Schulz (2012), *Das neue IT-Grundrecht – staatliche Schutzpflicht und Infrastrukturverantwortung,* Datenschutz und Datensicherheit (6), p. 395-400.

Schulzki-Haddouti 2017
C. Schulzki-Haddouti (2017), *Ideengeschichte des Privacy by Design,* datenschutzbeauftragter-online.de 12 april 2017.

SCP 2017
R. Bijl, J. Boelhouwer en A.Wennekers (2017), *De Sociale Staat van Nederland,* Den Haag: SCP

Selznick 1992
P. Selznick (1992), *The Moral Commonwealth: Social Theory and the promise of community,* University of California Press.

Sen 1984.
A. Sen (1984), *Rights and Capabilities.* In: *Resources, Values and Development,* Cambridge, Mass: Harvard University Press.

Simitis 1998
S. Simitis (1998), *Datenschutz - Rückschritt oder Neubeginn*, NJW, p. 2475.

Slob & Schilte 2014
M. Slob en E. Schilte (2014), *Mensenrechten in beweging. Privacy,klimaatverandering en internationale rechtsorde,* Amsterdam.

Solove, 2006
D.J. Solove (2006), *A Taxonomyof Privacy,* University of Pennsylvania Law Review, 154, nr. 3.

Solove 2007
D. Solove (2007), *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy,* San Diego Law Review, p. 745-772.

Solove 2013
D.J. Solove (2013), *Introduction: Privacy Self-management and the Consent Dilemma,* Harvard Law Review, p. 126.

Sloot 2017
B. Sloot (2017), *Privacy As Virtue: Moving Beyond the Individual in the Age of Big Data*.

Sloot 2018
B. Sloot (2018), *AVG in gewone mensentaal,* Amsterdam University Press.

Smit 2014
G. Smit (2014), *Opening the Black Box: The Work of Watching,* Abingdon, Oxon: Routledge.

Somsen 2006
H. Somsen (2006), *Regulering van humane genetica in het neo-eugenetische tijdperk (oratie)*.

Spronken & Koopmans 2017
T.N.B.M Spronken en P.C. Koopmans, (2017), *Gedeelde informatie, over de naleving van de wet door het openbaar ministerie bij het toevoegen van strafvorderlijke, justitiële en politiële gegevens aan het Bopz-dossier, rapport van de procureur-generaal bij de Hoge Raad der Nederlanden in het kader van het in artikel 122 lid 1 Wet RO bedoelde toezicht,* Den Haag.

Staatscommissie Grondwet, Den Haag, november 2010, p. 81.

Steen & Hajer 2014
M. van der Steen, M. Hajer e.a. (2014), *Leren door Doen, Overheidsparticipatie in een energieke samenleving,* NSOB.

Steijn 2014
W. Steijn (2014), *Developing a sense of privacy: comparison of adolescents', young adults', and adults' behaviour on social network sites and their privacy concerns*.

Stiftung Datenschutz 2017
Foundation for Data Protection, 'New ways of providing consent in data protection – technical, legal and economic challenges', stiftungdatzenschutz.org 12 april 2017.

Stiggelbout 2012
A.M. Stiggelbout, M.P.T. De Wit, D. Frosch, F. Légaré, V.M. Montori, L. Trevena, G. Elwyn (2012), *Shared decision making: really putting patients at the centre of healthcare,* BMJ 2012;344:e256 doi: 10.1136/bmj.e256.

Stiggelbout 2015
A.M. Stiggelbout, A.H. Pieterse, J.C.J.M. De Haes (2015), *Shared decision making: Concepts, evidence, and practice,*Patient Education and Counseling, 98: 1172-9.

Struik 2017
H. Struik (2017), *AVG: What'sold?,* P&I158, nr. 4, (transponeringstabel AVG – Richtlijn 95/46/EG – Wbp)

Stuurman 2009
C. Stuurman (2009), *Annotatie bij rechtbank Den Haag 31 december 2008 (Knooble/Staat en NNI)*.

Stuurman, 2017
C. Stuurman (2017), *The digitisation driven impact of data protection regulation on the standardization process, in:* Jakobs, K. (ed.), (The EURAS Board Series), 28 Jun 2017 Proceedings 22nd EURAS Annual Standardisation Conference: Digitalisation: Challenge and Opportunity for Standardisation.Aachen: Verlagshaus Mainz GmbH Aachen, p. 337-350 14 (Taeger 1983 J. Taeger, Die Volkszählung, 1983).

Thaler & Sunstein 2008
R. Thaler en C. Sunstein (2008), *Nudge. Naar betere beslissingen over gezondheid geluk en welvaart,* Business Contact.

Thole 2010
E. Thole e.a. (red.) (2010), *50 Vragen over privacy,* Deventer: Kluwer, p. 150-153.

Time 2006, "You, Person of the Year".

Timmer 2013
W. Timmer (2013), *Zorgplichten aan het werk*, RegelMaat, 28, nr. 6.

Tjong Tjin Tai 2015
T.F.E. Tjong Tjin Tai (2015), *Duties of care and diligence against cybercrime,* Tilburg University.

TNO 2015, *Privacybeleving op het internet in Nederland*.

Topol 2015
E. Topol (2015), *The Patiënt will see you know, the future of medicine in your hands,* New York: Basic Books.

Trubek 1984
D. Trubek (1984), *Where the action is: critical Legal studies and empiricism,* Stanford Law Review, 36: p. 572-622.

Van Alesenoy, Kosta & Dumortier 2014
B. Alesenoy, E. Kosta, J. Dumortier (2014), *Privacy notices versus informational self-determination: Minding the gap,* 28 International Review of Law, Computers & Technology.

Van Beers 2009
B.C. van Beers (2009), *Persoon en lichaam in het recht, menselijke waardigheid en zelfbeschikking in het tijdperk van de medische biotechnologie,* Den Haag: Boom Juridische uitgevers, 775.

Van Blarkom, Borking, Olk 2003
G.W. van Blarkom, J.J. Borking, J.G.E. Olk (2003), *Handbook of Privacy and Privacy-Enhancing Technologies: The case of intelligent software agents,* Den Haag.

Van den Bergh 1969
J.H. van den Bergh (1969), *Medische macht en medische ethiek*.

Van de Bunt & Strijbos 2018
T. van de Bunt en A. Strijbos (2018), *De bewerkersovereenkomst onder de AVG*, NJB 2018, 357.

Van Dijck & José 2014
Van Dijck, José (2014), *Datafication, dataism and datasurveillance: Big Data between scientific paradigm and ideology,* Surveillance & Society, 12 (2): 197-208.

Van Dijk 2006
P. van Dijk et al. (2006), *Theory and Practice of the European Convention on Human Rights*, p. 664 e.v.

Van Est 2014
R. van Est, V. Rerimassie, I. van Keulen en G. Dorren (2014), *Intieme technologie: De slag om ons lichaam en gedrag,* Den Haag.

Van den Hoven & Manders-Huits 2006
J. van den Hoven en N. Manders-Huits (2006), *Identiteitsmanagement en morele identificatie*, Algemeen Nederlands Tijdschrift voor Wijsbegeerte.

Van Lieshout 2012
M. Van Lieshout e.a. (2012), *Stimulerende en remmende factoren van Privacy by Design in Nederland, TNO-rapport 2012,*Delft: TNO.

Van der Pot 2006
C.W. van der Pot (2006), *Handboek Van Het Nederlandse Staatsrecht*, Deventer: Kluwer 2006.

Verberk 2011
S. Verberk (2011), *Probleemoplossend strafrecht en het ideaal van responsieve rechtspraak,* Den Haag: Sdu Uitgevers.

Verbruggen & Wolters 2017
P.W.J. Verbruggen en P.T.J. Wolters (2017), *Consument en cybersecurity. Een agenda voor Europese harmonisatie van zorgplichten,* TvC, nr. 1.

Verbruggen & Wolters 2017
P.W.J. Verbruggen e.a. (2017) , *Towards Harmonised Duties of Care and Diligence in Cybersecurity,* European Foresight Cyber Security Meeting 2016. Den Haag: Cyber Security Council 2016.

Verdonschot 2013
J.H. Verdonschot, *Sharing rules that work: developing law as practical and concrete guidelines for fair sharing (proefschrift),* Tilburg, 2013.

Vereniging voor wetgeving en wetgevingsbeleid 1995
F. Plate, JA. Smit e.a. (1995), *De wet, instrument en waarborg? Verslag van het symposium, gehouden op 31 maart 1995 ter gelegenheid van de algemene ledenvergadering van de Vereniging voor wetgeving en wetgevingsbeleid: met preadviezen van F. Plate, J.A. Smit.*

Verhelst 2012
E.W. Verhelst (2012), *Recht doen aan Privacyverklaringen. Een juridische analyse van privacyverklaringen op internet (dissertatie),* Universiteit Tilburg, Deventer: Kluwer.

Verhelst, 2017
E.W. Verhelst (2017), *Blockchain aan de ketting van de Algemene verordening gegevensbescherming?,* P&I 3, nr. 1.

Verhey 1992
L.F.M. Verhey (1992), *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy,* W.E.J. Tjeenk Willink & NISER.

Vermesan & Friess 2011
O. Vermesan en P. Friess (2011), *Internet of Things, Global Technological and Societal Trends, Smart Environments and Spaces to Green ICT,* River publishes.

Vermunt & Hooghiemstra 2015
N. Vermunt en T. Hooghiemstra (2015), *Naar een persoonlijk gezondheidsdossier dat werkt,* Lucide.

Vermunt e.a. 2017
N. P. Vermunt, M. Harmsen, G. Elwyn, G.P. Westert, J.Burgers, N.G. Olde Rikkert, M.Faber (2017), *A three-goal model for patients with multimorbidity: A qualitive approach,* Health Expectations, 28 november 2017.

Versmissen, Terstegge en Krijgsman 2017
K.Versmissen, J.Terstegge, N.Krijgsman (2017), *Grip op de AVG,* Deventer: Wolters Kluwer.

Vinke & Berghuis-van der Wijk 1975
P. Vinke, & I. Berghuis-van der Wijk (1975), *Rechtsregels in de ervaringswereld van verschillende bevolkingslagen,* Deventer: Kluwer.

Vogelsang 1987
K. Vogelsang (1987), *Grundrecht auf Informationelle Selbstbestimmung?,* p. 136 e.v.

Walzer 1983
M. Walzer, (1983), *Spheres of Justice, A Defense of Pluralism and Equality,* New York: Basic Books.

Warren & Brandeis 1890
S.D. Warren & L.D. Brandeis (1890), *The Right to Privacy,* Harvard Law Review (4), p. 193-220.

Weichert 2001
T. Weichert (2001), *Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung,* NJW, p. 1463.

Weichert 2008
T. Weichert (2008), *Verfassungsrechtliche Grundlagen des Datenschutzes*, in: W. Kilian & B. Heussen, *Computerrechts-Handbuch*.

Westin 1967
A.F. Westin (1967), *Privacy and Freedom,* London: The Boldly Head 1967, p. 7.

Weyers 1996
Weyers (red.) (1996), *De sociale werking van recht. Een kennismaking met de rechtssociologie en rechtsantropologie,* Nijmegen: Ars Aequi libri, p. 177-199.

Widlak & Peeters, 2018
A. Widlak en R. Peeters (2018), *De digitale kooi, (on)behoorlijk bestuur door informatiearchitectuur,* Den Haag: Boom Bestuurskunde.

Wieczorek 2011
M.A. Wieczorek (2011), *Informationsbasiertes Persönlichkeitsrecht. Überlegungen zur Restauration des Persönlichkeitsschutzes im Internetzeitalter*, Datenschutz und Datensicherheit (7), p. 476-481.

Wing 2016
L. Wing (2016), *Ethical Principles for Online Dispute Resolution. A GPS Device for the Field,* International Journal on Online Dispute Resolution (3) 1.

Witmer & de Roode (eindred.) 2004
J.M. Witmer, & R.P. de Roode (eindred.) (2004). *Van wet naar praktijk. Implementatie van de WGBO. Deel 2. Informatie en toestemming,* Utrecht, 2004.

Witteveen 2015
W.J. Witteveen (2015), *De wet als kunstwerk, een andere filosofie van het recht,* Den Haag: Boom Juridische uitgevers, tweede oplage.

Wolter & Dolan
J. Wolter en M.W. Dolan, *The Personal Health Record,* Chicago IL: AHIMA, American Health Information Management Association.

WRR 2011
Rapport iOverheid, 2011.

WRR 2014
Met kennis van gedrag beleid maken, augustus 2014

WRR 2016
L. Ottes (2016), *Big Data in de zorg, achtergrondstudie bij: WRR, Big Data in een vrije en veilige samenleving*.

WRR 2017
Weten is nog geen doen. Een realistisch perspectief op zelfredzaamheid.

Zeeuw, de 2017
J. de Zeeuw (2017), *Opmerkingen NGFG bij Richtlijnen voor functionarissen voor de gegevensbescherming van de Artikel 29-werkgroep,* P&I 109, nr. 3.

ZonMW 2013
Achtergrondstudies: Zelfbeschikking in de zorg. Te raadplegen via *ZonMw* zonmw.nl/publicaties.

Zuurmond 1994
A. Zuurmond (1994), *De Infocratie: een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk,* Delft.

Bijlage B *Rechtspraak*

Europees Hof voor de Rechten van de Mens

EHRM 6 september 1978 (*Klass e.a. t. Duitsland*)
EHRM 26 maart 1987 (*Leander t. Zweden*)
EHRM 25 maart 1983, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75 (Silver e.a. t. Verenigd Koninkrijk)
EHRM 2 augustus 1984, nr. 8691/79 (Malone)
EHRM 7 juli 1989 (*Gaskin t. VK*), NJCM-bulletin 1990, p. 206
EHRM 9 september 1992 (*Reyntjens t. België*)
EHRM 22 april 1993, *Modinos t. Cyprus*, nr. 15070/89. (*Modinos*)
EHRM 22 februari 1994 (*Burghartz t. Zwitserland*)
EHRM 12 maart 1994 (*T.V. t. Finland*)
EHRM 25 november 1994 (*Stjerna t. Finland*)
EHRM 25 februari 1997 (*Z. t. Finland*)
EHRM 27 augustus 1997, NJ 1999, 464 (*M.S. t. Zweden*)
EHRM 19 februari 1998 (Guerra et al. t. Italië)
EHRM 28 januari 2000 (*McGinley en Egan t. VK*)
EHRM 16 februari 2000 (*Amann t. Zwitserland*)
EHRM 7 februari 2002 (*Mikulic t. Kroatië*)
EHRM 29 april 2002, nr. 2346/02 (*Pretty t. het VK*)
EHRM 24 september 2002 (*M.G. t. VerenigdKoninkrijk*)
EHRM 28 januari 2003 (*Peck t. VK*)
EHRM 13 februari 2003 (*Odièvre t. Frankrijk*)
EHRM 24 juli 2003 (*Smirnova t. Rusland*)
EHRM 24 juni 2004 (*Caroline von Hannover t. Duitsland*)
EHRM 11 januari 2005 (*Sciacca t. Italië*)
EHRM 19 oktober 2005 (*Roche t. VK*)
EHRM 7 maart 2006, nr. 6339/05, (*Evans t. het VK) NJCM-Bulletin* 2006, p. 863 (m.nt. C.J. Forder & J. Whittingham), *GJ* 2006, 43 (m.nt. A.C. Hendriks), *EHRC* 2006, 47 (m.nt. E. Brems)
EHRM 15 mei 2006 (*Erven KrestenFiltenborgMortensen t. Denemarken*)
EHRM 30 mei 2006 (*Ebru & Tayfun Engin Colak*)
EHRM 29 juni 2006 (*Panteleyenko t. Oekraïne*)
EHRM 13 juli 2006 (*Jäggi t. Zwitserland*)
EHRM 5 oktober *2006* (*Trocellier t. Frankrijk)*
EHRM 10 oktober 2006, nr. 7508/02 (*L.L. t. Frankrijk*)
EHRM 12 april 2007 (*Uslu t. Turkije*)
EHRM 9 oktober 2007 (*K.H. et al t. Slowakije*)
EHRM 1 juli 2008 (*Daroczy t. Hongarije*)

EHRM 17 juli 2008, zaak 20511/03 (*I t. Finland*)
EHRM 25 november 2008 (*Biriuk t. Litouwen*)
EHRM 13 januari 2009, 37048/04 [2009] ECHR 63 (*GiorgiNikolaishvili t. Georgië*)
EHRM 2 juni 2009 (*Szuluk t. VK*)
EHRM 2 juni 2009 (Codarcea t. Roemenië)
EHRM 7 december 2010 (*Andersson t. Zweden*)
EHRM 26 mei 2011, *R.R. t. Polen*, nr. 27617/04, § 197
EHRM 30 mei 2013, nr. 35985/09 (*Martin t. Estland*)

Hof van Justitie van de EU

HvJ EU 5 oktober 1994, zaak C-404/92, (*X t. Commissie*)
HvJ EU 9 oktober 2001, C-377/98, (*Nederland t. Parlement en Raad*)
HvJ EU 20 mei 2003, C-465/00 (*Österreichischer Rundfunk e.a.*)
HvJ EU 30 mei 2006, C-317/04 (*Uitwisselingluchtvaartpassagiersgegevens VS*)
HvJ EU 18 Juli 2007, C-275/06, (Promusicae vs. Telefónica de España)
HvJ EU 5 mei 2011 Zaak C-316/09, (*MSD Sharp & DohmeGmbH/MerckleGmbH*)
HvJ EU 5 mei 2011, Zaak C-543/09 (*Deutsche Telekom AG tegen Bundesrepublik Deutschland*)
HvJ EU 8 april 2014, C-293/12 en C-594/12 (*Digital RightsIreland en Seitlinger*)
HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (Google Spain/Costeja)
HvJ EU 6 oktober 2015, zaak C-362/14, (*Facebook/Schrems*), ECLI:EU:C:2015:650

Bundesverfassungsgericht (Constitutioneel Hof van Duitsland)

BVerfG 15 januari 1958, BVerfGE 7, 198 (204) (Lüth)
BVerfG 16 juli 1969, BVerfGE 27, 1 (Mikrozensus)
BVerfG 15 januari 1970, BVerfGE 27, 344 (Ehescheidungsakten)
BVerfG 8 maart 1972, BVerfGE 32, 373 (379) (Ärztliche Schweigepflicht).
BVerfG 14 februari 1973, BVerfGE 34, 269 (281) (Soraya).
BVerfG 5 juni 1973, BVerfGE 35, 202 (235 e.v.) (Lebach);
BVerfG 25 februari 1975, BVerfGE 39, 1 (Schwangerschaftsabbruch I)
BVerfG 16 oktober 1977, BVerfGE 46, 160 (Schleyer)
BVerfG 8 augustus 1978, BVerfGE 49, 89 (Kalkar I)
BVerfG 1 maart 1979, BVerfGE 50, 290 (336) (Mitbestimmung)
BVerfG 20 december 1979, BVerfGE 53, 30 (Mülheim-Kärlich)
BVerfG 3 juni 1980, BVerfGE 54, 148 (155) (Eppler)
BVerfG 28 juni 1983, BVerfGE 64, 261 (276 e.v.) (Hafturlaub)
BVerfG 15 december 1983, BVerfGE 65, 1 (Volkszählung)
BVerfG 20 juni 1984, BVerfGE 67, 157 (172) (G 10)
BVerfG 23 april 1986, BVerfGE 73, 261 (269) (Sozialplan)
BVerfG 13 mei 1986, BVerfGE 72, 155 (170 e.v.)
BVerfG 31 januari 1989, BVerfGE 79, 256 (268 e.v.) (Kenntnis der eigenen Abstammung)
BVerfG 14 september 1989, BVerfGE 80, 367 (373 e.v.) (Tagebuch)
BVerfG 10 november 1998, BVerfGE 99, 185 (193) (Scientology)
BVerfG 28 mei 1993, BVerfGE 88, 203 (Schwangerschaftsabbruch II)
BVerfG 24 juni 1993, BVerfGE 89, 69 (82 e.v.).

BVerfG 19 oktober 1993, BVerfGE 89, 214 (229) (Bürgschaftsverträge)
BVerfG 26 april 1994, BVerfGE 90, 263 (270 e.v.)
BVerfG 7 maart 1995, BVerfGE 92, 191 (Personalienangabe)
BVerfG 6 mei 1997, BVerfGE 96, 56 (63) (Vaterschaftsauskunft)
BVerfG 25 november 1999, NJW 2000, 1859
BVerfG 15 december 1999, BVerfGE 101, 361 (380) (Caroline von Monaco II)
BVerfG 14 december 2000, BVerfGE 103, 21 (Genetischer Fingerabdruck I)
BVerfG 14 december 2000, BVerfGE 103, 21 (Genetischer Fingerabdruck I).
BVerfG 9 oktober 2002, BVerfGE 106, 28 (35) (MithLSPörvorrichtung)
BverfG, 3 maart 2004, BVerfGE 109, 279 (311 e.v.) (Gro er Lauschangriff)
BVerfG 12 april 2005, BVerfGE 112, 304 (Global Positioning System)
BVerfG 25 oktober 2005, BVerfGE 114, 339 (346) (Mehrdeutige Meinungsäusserungen)
BVerfG 2 maart 2006, BVerfGE 115, 166 (182) (Kommunikationsverbindungsdaten)
BVerfG 4 april 2006, BVerfGE 115, 320 (Rasterfahndung II)
BVerfG februari 2007, BVerfGE 117, 202 (Vaterschaftsfeststellung)
BVerfG 27 februari 2008, BVerfGE 120, 274 (Online-Durchsuchungen)
BVerfG 11 maart 2008, BVerfGE 120, 378 (Automatisierte Kennzeichenerfassung)
BVerfG 17 februari 2009, BVerfGE 122, 342 (Bayerisches Versammlungsgesetz)
BVerfG 16 juni 2009, BVerfGE 124, 43 (Beschlagnahme von E-Mails)
BVerfG 2 maart 2010, BVerfGE 125, 260 (Vorratsdatenspeicherung)

Overige Duitse jurisprudentie

BGHZ 25 mei 1954, BGHZ 13, 334 (Veröffentlichung von Briefen)
BGHZ 31 oktober 1974, BGHZ 63, 196 (198) (Eingriff an Eigentum an Gemeindestra en)
BayVerfGH, DVBI, 2003,861
HambOVG, DÖV 2007,893 (Ls)
SächsOVG, NJW 2007,169 (170)
BVerwG, NJW 2008, 3081
BGH, BGHZ 171, 252 (256)

Hoge Raad

HR 21 april 1913, NJ 1913, 959
HR 22 juni 1973, NJ 1973, 386 (Fluoridering)
HR 19 november 1985, NJ 1986, 533, met annotatie van 't Hart (Verschoningsrecht)
HR 2 december 1988, NJ 1989, 752, m.nt. Maeijer, Computerrecht 1989, nr. 2, p. 104, m.nt. Kuitenbrouwer
HR 15 april 1994, NJ 1994, 608 (*Valkenhorst*), m.nt. Hammerstein-Schoonderwoerd
HR 23 november 2001, NJ 2002, 386 en 387, m.nt. Vranken, r.o. 3.5.2 (Dwarslaesie)
HR 29 juni 2007, LJN AZ4663 (Dexia), LJN AZ4664 (Dexia) en LJN BA3529 (Hollandse Bank-Unie)
HR 9 september 2011. LJN BQ8097. JPG 2011/186. (*Santander*)
HR 27 april 2012, LJN BV 1301 (*Beeldbrigade*)
HR 12 maart 2013, NJ 2013/424. (*Jomanda*)
HR 1 december 2017, ECLI:NL:HR:2017:3053 (LSP)

Afdeling Bestuursrechtspraak van de Raad van State

ABRvS 30 november 2011, m. nt. G. Overkleeft-Verburg
ABRvS 30 november 2011, ECLI:NL:RVS:2011:BU6383, JB 2012/44LJN BU6383. JPG 2012/8. JB 2012/44 (m.nt. Overkleeft-Verburg)

Hof

Hof Arnhem-Leeuwarden 8 maart 2016, ECLI:NL:GHARL:2016:1697

Rechtbanken

Rb Rotterdam 29 september 2010. LJN BN9944. JPG 2011/4
Rb Noord-Holland, 12 mei 2017 ECLI:NL:RBNHO:2017:3955
Rb Midden-Nederland 7 juli 2017, ECLI:NL:RBMNE:2017:3421
Rb Midden-Nederland 7 juli 2017, ECLI:NL:RBMNE:2017:3422
Rb Midden-Nederland 2 augustus 2017, ECLI:NL:RBMNE:2017:4011

Autoriteit Persoonsgegevens (voorheen CBP en Registratiekamer)

College bescherming persoonsgegevens aan de minister van VWS, d.d. 20 november 2006, kenmerk z2006-01388, advies inzake aanvulling Besluit gebruik burgerservicenummer in de zorg. Op internet: http://www.cbpweb.nl/downloads_adv/z2006-01388.pdf

College bescherming persoonsgegevens, *Zienswijze CBP over doorstartmodel voor landelijke uitwisseling medische gegevens*, 9 augustus 2011 en CBP *Rapport definitieve bevindingen Landelijk Schakelpunt,* d.d. 1 september 2014, kenmerk z2012-779

College bescherming persoonsgegevens. *Onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim door VCD Humannet B.V.* December 2014, kenmerk z2012-0028.8

Autoriteit Persoonsgegevens. *Rapport definitieve bevindingen NZa-DIS,* d.d. 13 september 2016, kenmerk z2015-00355.

Tuchtcolleges

CTG, 26 januari 2010. GJ 2010/38/ JPG 2010/81
RTC Amsterdam 2 november 2010. LJN YG0637. JPG 2011/24. GJ 2011/5 (m.nt. Y.M. Drewes en A.C. Hendriks)
CTG 12 april 2011. LJN YG1038. JPG 2011/101
RTC Groningen 7 juni 2011. LJN YG1163. JPG 2011/134
RTG 's-Gravenhage 5 juli 2011, LJN YG1213
RTC Eindhoven 13 juli 2011. LJN YG1222. JPG 2011/138
RTG Groningen 20 december 2011. LJN YG1629. JPG 2012/11
RTC Groningen, 8 mei 2012. LJN YG2012. JPG 2012/112
RTC Zwolle, 10 mei 2012. LJN YG2019. JPG 2012/113

Samenvatting

Introductie
Het begrip 'informationele zelfbeschikking' is al decennia geleden in de rechtspraak ontwikkeld, maar heeft – door een aantal samenhangende technologische vernieuwingen – een nieuwe kleur en karakter gekregen. Aanvankelijk was het vooral een 'defensief concept', maar door de introductie en massale verspreiding van *smartphones* en andere mobiele gegevensdragers krijgt het inmiddels een actief en assertief karakter. Gebruikers lijken steeds meer hun 'eigen' gegevens te kunnen beheren. Informationele zelfbeschikking lijkt daardoor daadwerkelijk binnen het bereik van zeer velen te komen.

Informationele zelfbeschikking is voor dit onderzoek gedefinieerd als het vermogen van een persoon om in beginsel zelf te bepalen in hoeverre persoonsgegevens worden gebruikt en verder bekendgemaakt, met het oog op een zelfbepaald leven. De mate waarin personen daadwerkelijk het vermogen hebben om zelf te bepalen in hoeverre persoonsgegevens over hen worden gebruikt, wordt beïnvloed door de opmars van persoonlijke gezondheidsomgevingen via mobiele gegevensdragers.

Vooral in de gezondheidszorg duiken nieuwe vragen op. Hoe zijn gezondheidsgegevens in deze nieuwe situatie met persoonlijke gezondheidsomgevingen adequaat te beschermen? Kan het medisch beroepsgeheim nog zijn beschermende werking hebben? Moet daarbij een onderscheid worden gemaakt naar de typen personen wiens gegevens het betreft? Wat moet de rol van de overheid en de rechtstreeks betrokken private partijen zijn? Welke rol kan en moet *privacy by design* spelen? Welke overige toekomstgerichte aanbevelingen zijn er – gelet op de opmars van persoonlijke gezondheidsomgevingen – te geven?
Op basis van de analyse in deze dissertatie kom ik tot de volgende conclusies, een stelling en aanbevelingen.

Conclusies
De eerste conclusie is dat het concept van 'informationele zelfbeschikking' in de rechtspraak en in juridische publicaties is ontwikkeld en door de introductie en massale verspreiding van mobiele gegevensdragers inmiddels een andere strekking krijgt. Het begrip informationele zelfbeschikking krijgt een actieve en assertieve lading doordat personen de keuzevrijheid en ontplooiingsmogelijkheden krijgen om zelf hun persoonsgegevens te (laten) beheren en dus ook zelf kunnen beslissen wat er met die persoonsgegevens gebeurt. Bovendien geeft nieuwe wet- en regelgeving in de Algemene verordening gegevensbescherming (AVG), de Uitvoeringswet AVG en de Wet aanvullende bepalingen verwerking

persoonsgegevens in de zorg (Wabvpz) aan personen steeds meer informationele zelfbeschikkingsrechten, zoals het recht op elektronische inzage, (gespecificeerde) toestemming en dataportabiliteit.

De tweede conclusie is dat recente maatschappelijke en technologische ontwikkelingen, leiden tot een systematische disbalans tussen de machtscapaciteit voor bedrijven en overheid enerzijds, en die van personen anderzijds. Het herstellen van deze disbalans is gewenst. In de praktijk blijkt dat gezondheidsgegevens worden verhandeld zonder dat personen daarvan op de hoogte zijn.

De derde conclusie is dat voor Duitsland – de bakermat van informationele zelfbeschikking – het recht op informationele zelfbeschikking mogelijk en wenselijk is binnen het Duitse rechtsstelsel. Informationele zelfbeschikking is in Duitsland een facet van het algemeen persoonlijkheidsrecht en het recht op menselijke waardigheid. Het recht op informationele zelfbeschikking alleen bood in Duitsland onvoldoende rechtsbescherming tegen inbreuk op informatiesystemen. Vandaar dat het Hof het 'computer-grondrecht' heeft geformuleerd dat beoogt bescherming te bieden tegen inbreuk op ingrijpen in informatiesystemen.

De vierde conclusie is dat in het Europese en Nederlandse recht er geen expliciet recht is op informationele zelfbeschikking, maar het wel impliciet bestaat. Zo is er Europese en Nederlandse wetgeving ter bescherming van persoonsgegevens op grond waarvan verwerkingsverantwoordelijke bedrijven en overheden plichten hebben en personen een aantal rechten. In de Nederlandse wetgeving zijn er aanvullende informationele zelfbeschikkingsrechten voor personen ten opzichte van zorgaanbieders, maar geen aanvullende rechten ten opzichte van andere verwerkingsverantwoordelijke bedrijven en overheden die gezondheidsgegevens verwerken via persoonlijke gezondheidsomgevingen. Meer aanvullende rechtsbescherming is wenselijk ten behoeve van meer informationele zelfbeschikking.

De vijfde conclusie is dat uit onderzoek is gebleken dat verschillende typen personen in de discussie over informationele zelfbeschikking juridische en morele aandacht nodig hebben, zoals:

– personen die zich zorgen maken over machtsmisbruik;
– personen die gegevens niet kunnen of willen 'managen', en;
– personen die actief zelf persoonsgegevens willen 'managen'.

De zesde conclusie is dat bij de komst van persoonlijke gezondheidsomgevingen (via websites en apps) het medisch beroepsgeheim – dat van oudsher voor medische dossiers geldt – vrijwel geen rechtsbescherming meer biedt. Er is kortom behoefte aan aanvullende regulering om personen actief te beschermen.

De zevende conclusie is dat normering ook gestalte blijkt te kunnen krijgen in de applicaties zelf, via *privacy by design*. Bij het faciliteren van persoonlijke gezondheidsomgevingen betekent dit concreet dat personen de keuzevrijheid

kunnen krijgen om op elk gewenst moment *real time* toegang te krijgen tot hun gezondheidsgegevens. Daarnaast kan een speciale digitale butler personen beschermen in de complexe big-datasamenleving. In de algoritmen van de digitale butler kunnen per persoon en per context specifieke voorwaarden en voorkeuren worden opgenomen.

Stelling
Op basis van de analyse in deze dissertatie is mijn stelling dat door de geschetste ontwikkelingen de machtscapaciteit van bedrijven en overheden over gezondheidsgegevens groeit. Deze groeiende machtscapaciteit van bedrijven en overheden behoeft een vorm van tegenmacht. Met het oog op deze ontwikkelingen, waaronder de opmars van persoonlijke gezondheidsomgevingen, zijn de volgende aanbevelingen te geven.

Aanbevelingen

1. Afsprakenstelsel MedMij
Het in ontwikkeling zijnde Nederlandse Afsprakenstelsel MedMij voor persoonlijke gezondheidsomgevingen is bedoeld om bij te dragen aan informationele zelfbeschikking voor de gebruikers van de persoonlijke gezondheidsomgevingen.

Daarbij moet in het Afsprakenstelsel MedMij de persoon ten opzichte van de leverancier van persoonlijke gezondheidsomgevingen en de samenleving worden beschermd door te benadrukken dat de persoon geen verwerkingsverantwoordelijke is in de zin van de AVG. De kern is dat de aanbieder van de persoonlijke gezondheidsomgeving in de zin van de AVG een verwerkingsverantwoordelijke is met plichten en de persoon, als gebruiker, rechten heeft. Indien MedMij onvoldoende rechtsbescherming blijkt te bieden, lijkt op dat moment aanvullende wet- en regelgeving aan de orde. Als blijkt dat het Afsprakenstelsel MedMij onvoldoende rechtsbescherming biedt, dienen de toezichthouders in te grijpen. Daarbij is een effectieve taakverdeling tussen de toezichthouders aan te bevelen.

2. Online dispute resolution
Gegeven de specifieke context van online persoonlijke gezondheidsomgevingen beveel ik verschillende vormen van *online dispute resolution* (ODR) in combinatie met menselijke geschiloplossers aan. Bij persoonlijke gezondheidsomgevingen zijn voor verschillende typen van geschillen onderscheidende vormen van menselijke geschiloplossers in te zetten. Allereerst zijn er geschillen tussen een verwerkingsverantwoordelijke leverancier van persoonlijke gezondheidsomgevingen en een persoon als gebruiker hiervan. Bij dergelijke geschillen ligt ODR in combinatie met een ombudsfunctie of een mediator het meest voor de hand. Een ombudsfunctie is het meest laagdrempelig in het geval van een relatief eenvoudige klacht. Een speciale mediator voor conflicten rond persoonlijke gezondheidsomgevingen ligt meer voor de hand indien beide partijen er niet uitkomen en samen besluiten dit aan een mediator voor te leggen.
Bij geschillen tussen de gebruiker van een persoonlijke gezondheidsomgeving en zorgaanbieders ligt een informatievertrouwenspersoon meer voor de hand, vanwege de mogelijk gewenste zorgcontextspecifieke begeleiding. Bovendien

kan een informatievertrouwenspersoon helpen bij het indienen van een klacht bij de onafhankelijke klachtencommissie die voor zorgaanbieders bestaat.

3. Goede kennisbasis rechtspraak
De ontwikkeling van digitale persoonlijke gezondheidsomgevingen alsmede het type gegevens dat hierbij wordt gebruikt en de mogelijk kwetsbare positie van gebruikers van dergelijke omgevingen, toont het belang van een goede kennisbasis binnen de rechtspraak aangaande de kenmerken en consequenties van digitalisering.
Toegang tot de rechter en toezichthouders is juist bij persoonlijke gezondheidsomgevingen noodzakelijk.

4. Meer en andere menskracht Autoriteit Persoonsgegevens
De Autoriteit persoonsgegevens (AP) heeft meer en andere menskracht nodig. Vanuit de maatschappij, de rechtspraak en straks ook met de uitbreiding van verantwoordelijkheden en bevoegdheden door de AVG wordt van de AP een strengere rol op het terrein van handhaving verwacht. Op grond van de bevindingen in deze dissertatie betoog ik dat de AP meer en andere menskracht (bijvoorbeeld algoritmisten) moet krijgen.

5. Patiëntgeheim
Een wettelijke zwijgplicht voor verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen buiten de behandelrelatie wordt bepleit. Een dergelijk patiëntgeheim dient gepaard te gaan met een verschoningsrecht voor leveranciers en gebruikers van persoonlijke gezondheidsomgevingen wanneer zij voor de rechter komen te staan.

Zoals de Wabvpz te beschouwen is als een aanvulling op de AVG voor elektronische uitwisselingssystemen van zorgaanbieders die binnen de zorg gezondheidsgegevens verwerken, zo kan via nog te formuleren wetgeving wellicht de zwijgplicht als geheimhoudingsplicht voor verwerkingsverantwoordelijken van persoonlijke gezondheidsomgevingen geregeld worden.

Om het 'patiëntgeheim' voor gegevens in gezondheidsomgevingen net zo te regelen als het medisch beroepsgeheim, is naast deze geheimhoudingsplicht voor de leverancier een nieuw verschoningsrecht geboden bij de herziening van artikel 218 Wetboek van Strafvordering. Ook zal geregeld moeten worden dat het niet alleen natuurlijke, maar ook rechtspersonen zijn die zich erop kunnen beroepen.

6. Verbod op commercieel exploiteren van gezondheidsgegevens
Tot slot bepleit ik dat er een verbod moet komen op het commercieel exploiteren van gezondheidsgegevens. Zoals ook het verhandelen van organen verboden is op grond van de Wet orgaandonatie. De meerwaarde van een wettelijk verbod op handel in gezondheidsgegevens staat gelet op de datamacht van bedrijven buiten kijf. Hoe dit verbod precies zal moeten worden uitgewerkt, behoeft nader onderzoek. Toestemming op grond van de AVG is een cruciale voorwaarde voor informationele zelfbeschikking, maar biedt onvoldoende garanties.

Tot besluit

Het onderwerp van deze dissertatie betreft 'werk in uitvoering'. We zitten midden in een stroom die vaak turbulent is. Er ontstaan nieuwe vormen van informatiemacht die vragen om tegenmacht en om een helder juridisch en moreel kader om ontsporingen te voorkomen. Aan die opdracht heb ik gewerkt. Graag verdedig ik het hier geschetste perspectief en ben ik bereid het aan te passen wanneer er goede argumenten zijn.

Summary

Introduction
The concept of 'informational self-determination' was developed in the judicial system decades ago, but – through a number of interrelated technological innovations – it has changed colour and nature. Initially it was mainly a 'defensive concept', but due to the introduction and mass distribution of smartphones and other mobile data carriers, it is now getting an active and assertive character. Users increasingly govern their 'own' data. Informal self-determination, therefore, seems to be realistically within the reach of a large number of people.

For the purpose of this study, informal self-determination has been defined as the ability of a person to, in principle, determine for themselves which personal data are used and subsequently disclosed, with a perspective on a self-determined life. The extent to which individuals have the ability to determine the degree to which personal data about them are used is influenced by the increase of personal health environments via mobile data carriers.

In particular, new questions arise within the health care sector. How can health data be adequately protected by personal health environments in this new context? Can the duty of professional confidentiality still have its protective effect? Should a distinction be made in this respect between the types of people whose data it concerns? What should be the role of the public authorities and the private parties directly involved? What role can and should *privacy by design* play? What other forward-looking recommendations can be given – in view of the advancement of personal health environments?
Based on the analysis in this thesis, I come to the following conclusions, proposition and recommendations.

Conclusions
The first conclusion is that the concept of informational self-determination was developed in the judicial system and legal publications, but has now changed in purport as a result of the introduction and mass distribution of mobile data carriers. Informational self-determination has taken on a bold overtone as individuals are given the freedom of choice and personal development opportunities to (let them) manage their own personal data, and so decide for themselves what happens to this data. Moreover, new legislation and regulations in the General Data Protection Regulations (GDPR), the associated implementation act and the Processing of Personal Data in Healthcare (Additional Provisions) Act are giving individuals progressively more informational self-determination rights, such as the right to electronic inspection, (specified) consent and data portability.

My second conclusion focuses on recent social and technological developments that led to a systematic imbalance between the power capacity of companies and government on the one hand, and that of individuals on the other. Restoring this imbalance is desirable. In practice, it appears that health data are traded without people being aware of it.

Thirdly, it appears that for Germany – the cradle of informational self-determination – the right to it is both possible and desirable within the national legal system. In Germany, informational self-determination is a facet of the general personality freedom and the right to human dignity. The mere privilege to informational self-determination did not provide sufficient legal protection against infringements of information systems in Germany. That is why the Court of Appeal has formulated the 'fundamental rights of computer users' that intends to offer protection against such infringements.

The fourth conclusion is that there is no explicit right to informational self-determination in European and Dutch law, but that it does exist implicitly. For example, there is European and Dutch legislation on the protection of personal data under which processing companies and authorities have obligations, whereas individuals have a number of rights. In Dutch legislation, there are additional informational self-determination rights for individuals vis-à-vis healthcare providers, but no additional rights with other processing companies and governments that process health data via personal health environments. Further additional legal protection is worthwhile in the interest of more informational self-determination.

A fifth conclusion I have found is that research has revealed various types of people involved in the discussion on informational self-determination that require legal and moral attention, such as

- individuals who are worried about abuse of power;
- individuals who cannot or do not wish to 'manage' data, and;
- individuals who want to actively 'manage' personal data themselves.

Furthermore, a sixth conclusion stems from the advent of personal health environments (via websites and apps), where medical confidentiality – which traditionally applies to medical files – no longer provides any legal protection. In short, there is a need for supplementary regulation to actively protect individuals.

Finally, standardisation can apparently also take shape in the applications themselves, via *privacy by design*. In the facilitation of personal health environments, this means, more specifically, that people can have the freedom of choice to access their health data at any *real time*. Moreover, a special digital butler can protect people in the complex big data society. For each person and context, specific conditions and preferences can be included in the digital butler's algorithms.

Proposition
I propose that the developments outlined above are increasing companies' and governments' power capacity over health data, based on my previous analysis. This growing power capacity requires a form of counterforce. In view of these developments, including the growth of personal health environments, the following recommendations can be made.

Recommendations

1. MedMij Framework of Agreements
The Dutch MedMij Framework of Agreements for personal health environments, which is currently being developed, is intended to contribute to informational self-determination for the users.

In this framework, the individual must be protected in respect of the supplier of personal health care environments and society by emphasising that the individual is not a data controller as described in the GDPR. The heart of the matter is that within the meaning of the GDPR, the provider of the personal health environment is a data controller with obligations and that the individual, as a user, has rights. If the framework is found to provide insufficient legal protection at any time, further legislation and regulations should be placed on the agenda. If this turns out to be the case, the supervisory authorities must intervene. In doing so, an effective division of tasks between the supervisory authorities is advisable.

2. Online Dispute Resolution
Given the specific context of online personal health environments, I recommend various forms of *online dispute resolution* (ODR) in combination with human dispute resolvers. When it comes to personal health environments, various forms of human dispute resolvers can be employed for different types of disputes. First of all, there can be conflicts between a data controlling supplier of personal health care environments and a person who uses them. In such disputes, ODR in combination with an ombudsperson or a mediator is the most obvious option. With a relatively simple complaint, an ombudsperson is the most accessible official. A special mediator for conflicts concerning personal health environments is more likely if the parties fail to reach an agreement and jointly decide to submit the issue to a mediator.
In the event of friction between the user of a personal health environment and care providers, a confidential information counsellor is more necessary, due to the possibly desired care context-specific support. A confidential information counsellor can also help to file a complaint with the existing independent complaints committee for healthcare providers.

3. Adequate Knowledge Base within the Judicial System
The development of digital personal health environments, as well as the type of data used and the potentially vulnerable position of users of such environments, shows the importance of a good knowledge base within the judicial system with regards to the characteristics and consequences of digitisation.

Access to courts and supervisory authorities is required, especially when personal health environments are concerned.

4. More and Different Manpower for the Dutch Data Protection Authority (Dutch DPA)
The Dutch DPA needs a larger amount of, and variation in, manpower. Society and the judicial system expect the Dutch DPA to play a more stringent role in the area of enforcement, and this will increase in the near future with the upcoming expansion of responsibilities and powers under the GDPR. Based on the findings in this thesis, I argue that the Dutch DPA must be given more, and different, manpower (e.g. algorithmists).

5. Patient Confidentiality
I plead for a legal duty of confidentiality for controllers of personal health environments outside the treatment relationship. Such patient confidentiality should go together with the right of both the suppliers and users of personal health environments to refuse to give evidence when they are brought to justice.

Just as the Processing of Personal Data in Healthcare (Additional Provisions) Act can be seen as an addition to the GDPR for electronic exchange systems of care providers who process health data within the healthcare system, so might the duty of confidentiality for controllers of personal health environments perhaps be arranged through legislation that has yet to be formulated.

In order to arrange for 'patient confidentiality' for health environments in the same way as medical confidentiality, the revision of Article 218 of the Code of Criminal Procedure has provided a new right to refuse to give evidence in addition to the provider's duty of confidentiality. It will also be necessary to ensure that not only natural, but also legal persons can refer to them.

6. Prohibition of Commercial Exploitation of Health Data
Finally, I argue for a legal prohibition on the commercial exploitation of health data, similar to prohibition on the trade of organs under the Organ Donation Act. The added value of a legal prohibition on the trade in health data is beyond dispute, given companies' data power. How exactly this prohibition should be fleshed out will require further investigation. Consent under the GDPR is a crucial condition for informational self-determination, but does not offer adequate guarantees.

In conclusion
The subject of this thesis is 'work in progress'. We are sailing an often turbulent stream. New forms of information power are emerging, which call for counterforce and a clear legal and moral framework to prevent derailments. I worked towards answering this call. I look forward to defending the perspective that I have outlined here and I am open to revision if good arguments are put forth.

Dankwoord

In dit dankwoord probeer ik de vele familieleden, vrienden, inspiratoren en collega's die me tijdens de lange reis op weg naar deze dissertatie hebben geholpen, zoveel mogelijk persoonlijk te bedanken. Dankjewel:

Janneke & Sofie.

Paranimfen: Bas van Rheenen en Neeltje Vermunt.

Promotoren: Pieter Ippel en Corien Prins.

Eerdere promotor: Han Somsen.

Promotiecommissie: Maurice Adams, Colette Cuijpers, Hans Franken, Sjaak Nouwt en Kees Stuurman.

Student-assistenten: Kay Rommerts, Niels Rijke en Joanne Eenennaam.

Meelezers en -denkers: John Borking, Pieter Fokkink, Emilie van Hasselt, Peter Hustinx, Peter Kits, Mariette Lokin, Ad van Loon, Bert Niemeijer, Bettine Pluut, Ulco van de Pol, Wouter Steijn, Suzanne Verberk en Jin Ho Verdonschot.

Mede-auteurs van artikelen en rapporten in relatie tot het proefschrift: Rachel Gerards, Anja van der Heijde, Bert Arnolds. Jacqueline Krabben, Jaap-Henk Hoepman, Hester de Vries, Evert-Ben van Veen en Berber Wierstra.

Buitenpromovendi-groepje van Pieter Ippel: Albert van Steenbergen en Eric van den Luijtgaarden.

Proefschriftgroepje HEC/PBLQ: Victor Bekkers (wetenschappelijke leiding), Leo Smits (directeur), Dirk Schravendeel, Evert-Jan Mulder, Lauran Mathijssen en Marcel Bom.

Collega's van HEC & PBLQ, in het bijzonder taalpurist en kritische tegen-lezer Matthijs Kerkvliet, directeuren: Leo Smits, Philip Hennemann, Patty Heemskerk en Richard van Breukelen, collega-MT-leden, marketing: Laura Wijnants, Carlijne van de Burg, vormgeving: Paul Meijers, secretariaat, in het bijzonder Manouck Boone.

Collega's van RVZ & RVS, in het bijzonder de voorzitters Rien Meijerink en Pauline Meurs, de raadsleden betrokken bij de adviezen Patiënteninformatie en Consu-

menten eHealth: Didi Braat, Anke van Blerck-Woerdman, Henk Bosma, Wim Groot, Johan Mackenbach, Marjanne Sint, Dick Willems, Jan Kremer, Daan Dohmen, Greet Prins en de teamgenoten bij beide adviezen, in het bijzonder: Neeltje Vermunt, Marina de Lint, Leo Ottes en Marieke ten Have.

Het CEG, in het bijzonder Alies Struijs.

Inspiratoren: Maurits Barendregt, Annelien Bredenoord, Marlies van Eck, Sjef Gevers, Bart Jacobs, Aart Hendriks, Johan Legemaate, Hielke Hijmans, Mireille Hildebrandt, Jeroen van den Hoven, Lokke Moerel, Judith van Erp en Corrette Ploem.

Opgedane inspiratie in samenwerking met de programmateams van MedMij en Gespecificeerde Toestemming Patiëntenfederatie Nederland, in het bijzonder Marcel Heldoorn.

Inspectie Gezondheidszorg en Jeugd, in het bijzonder Johan Krijgsman.

NEN, in het bijzonder Shirin Golyardi en Rene Gouwens.

Redactie en Redactieraad ICTenhealth, in het bijzonder Thom Xhofleer, José Coenders en Lea Bouwmeester.

Redactie Smarthealth, in het bijzonder Jan en Frederieke Jacobs.

Redactie Journaal Bescherming Persoonsgegevens (JBP).

Sdu: Annemarie Arts, Marleen Schouten, Ivo Schouten en Katherine Tabak.

Secretariaat Universiteit Tilburg: Hanny Pentinga, Marga Verdonschot en Jacqueline Wayers.

Engelse vertaling: Els Spin.

Mijn familie – in het bijzonder mijn ouders Dinie en Frans, broer Frans en zus Paula, vrienden en collega's die begrip toonden en mij steunden, ook tijdens mijn (te) vele afwezigheid.

Trefwoordenregister